

## 明細書

## コンピュータシステムおよびそのアクセス権設定方法

5

## 技術分野

本発明は、コンピュータシステムおよびそのアクセス権設定方法に関し、特に、クライアントコンピュータからネットワークを介してサーバコンピュータにアクセスする際のセキュリティを確保する技術に関する。

10

## 背景技術

現在、コンピュータは、ネットワークを用いて相互に接続して利用するのが一般的であり、企業のみならず、一般家庭においても、ハブ、LANスイッチ、ルータなどを組み込んだネットワーク網の構築が行われるようになってきている。通常、企業では、社内LANやWANといった専用のネットワーク網を構築し、このネットワーク網に、各事業部の業務形態に合わせて、種々の機能をもったサーバコンピュータを接続して用いるのが一般的である。個々の社員は、このネットワーク網にパソコンなどのクライアントコンピュータを接続し、サーバコンピュータとデータのやりとりを行いながら業務を遂行することになる。

このようなネットワーク網を利用したコンピュータシステムを運用する上では、セキュリティの管理が非常に重要である。すなわち、ネットワーク網に接続された各コンピュータを、外部のハッカーによる不正アクセスから防御することはもちろんのこと、同一企業に所属する社員であっても、その所属や職責に応じて、それぞれ固有のアクセス制限を課するような運用が不可欠になる。

そこで、ネットワーク網を利用したコンピュータシステムにおけるセキュリティ管理の技術が種々提案されている。たとえば、特開2000-10930号公報および特開2003-122635号公報には、クライアントコンピュ

ータとサーバコンピュータとがネットワーク接続されているコンピュータシステムにおいて、個々のユーザごとにそれぞれ固有のアクセス権の管理を行うための技術が開示されている。

前掲の特許公報に開示されている技術をはじめ、従来のセキュリティ管理の手法は、いずれも個々のユーザごとに所定のアクセス権を設定する、という基本的な考え方に基づいている。すなわち、各ユーザにそれぞれ所定のアカウント（ユーザ名）とパスワードを付与し、個々のアカウントについてそれ所定のアクセス権の設定を行っておき、特定のアカウントによるログイン手続があった場合には、パスワードの照合によりこのログイン手続が正規のものであることを確認した後、当該アカウントに設定されているアクセス権の範囲内でアクセスを許可する、という運用を行うのが一般的である。

このように個々のユーザごとに特定のアクセス権を設定する、という基本方針は、大局的な見地からは、非常に合理的な手法であるが、コンピュータシステムを利用した業務形態の内容が益々複雑化する昨今では、必ずしもこのような基本方針だけでは対応しきれないことも少なくない。特に、多数の社員をかかえる企業では、不正な行為を行う社員の存在を完全には否定することができないので、個々の社員を完全に信頼して、どのような状況下においても無条件に同一のアクセス権を与えてしまうことは危険である。

そこで本発明は、個々のユーザに対して、状況に応じて（利用するコンピュータやネットワーク環境に応じて）、異なるアクセス権を設定することが可能なコンピュータシステムを提供することを目的とする。

### 発明の開示

(1) 本発明の第1の態様は、ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、このクライアントコンピュータに接続して用いるため

に個々のユーザに発行された携帯可能情報記録媒体と、を備えるコンピュータシステムにおいて、

各クライアントコンピュータに、それぞれ他のクライアントコンピュータと識別可能な固有の識別コードを記録しておき、

5 各携帯可能情報記録媒体に、それぞれ特定のクライアントコンピュータに記録されている特定の識別コードに対応する識別コードを記録しておき、

各クライアントコンピュータには、携帯可能情報記録媒体を接続するためのインターフェイス手段と、現在接続中の携帯可能情報記録媒体に記録されている識別コードと自分自身に記録されている識別コードとを照合する識別コード

10 照合手段と、この照合結果に基づいて所定のアクセス権を設定するアクセス権設定手段と、設定されたアクセス権の範囲内でサーバコンピュータに対するアクセスを行うサーバアクセス手段と、を設けるようにしたものである。

(2) 本発明の第2の態様は、ネットワーク網と、このネットワーク網に接続

されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライ

15 アントコンピュータと、このクライアントコンピュータに接続して用いるために個々のユーザに発行された携帯可能情報処理装置と、を備えるコンピュータシステムにおいて、

各クライアントコンピュータに、それぞれ他のクライアントコンピュータと識別可能な固有の識別コードを記録しておき、

20 各携帯可能情報処理装置に、それぞれ特定のクライアントコンピュータに記録されている特定の識別コードに対応する識別コードを記録しておき、

各クライアントコンピュータには、携帯可能情報処理装置を接続するためのインターフェイス手段と、現在接続中の携帯可能情報処理装置から伝達されてきたアクセス権の範囲内でサーバコンピュータに対するアクセスを行うサーバ

25 アクセス手段と、を設け、

携帯可能情報処理装置には、現在接続中のクライアントコンピュータに記録

されている識別コードと自分自身に記録されている識別コードとを照合する識別コード照合手段と、この照合結果に基づいて所定のアクセス権を設定するアクセス権設定手段と、設定されたアクセス権を現在接続中のクライアントコンピュータに伝達するアクセス権伝達手段と、を設けるようにしたものである。

5 (3) 本発明の第3の態様は、上述の第1または第2の態様に係るコンピュータシステムにおいて、

アクセス権設定手段が、照合結果が一致した場合には第1のアクセス権を設定し、照合結果が一致しなかった場合には第1のアクセス権よりも制限事項の多い第2のアクセス権を設定するようにしたるものである。

10 (4) 本発明の第4の態様は、上述の第1～第3の態様に係るコンピュータシステムにおいて、

クライアントコンピュータに内蔵されているLAN通信回路に付与されたMACアドレス、クライアントコンピュータの記憶装置に格納されている固有のデータ、もしくは、クライアントコンピュータの記憶装置に格納されているアプリケーションプログラムの構成を示す情報を、当該クライアントコンピュータを識別するための固有の識別コードとして用いるようにしたるものである。

15 (5) 本発明の第5の態様は、ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、このクライアントコンピュータに接続して用いるために個々のユーザに発行された携帯可能情報記録媒体と、を備えるコンピュータシステムにおいて、

各携帯可能情報記録媒体に、それぞれクライアントコンピュータをネットワーク網の特定箇所に接続した場合に得られる特定のネットワーク環境を示す環境情報を記録しておき、

20 各クライアントコンピュータに、携帯可能情報記録媒体を接続するためのインターフェイス手段と、現在接続中の携帯可能情報記録媒体に記録されている

環境情報によって示されるネットワーク環境と自分自身の現在のネットワーク環境とを照合する環境照合手段と、この照合結果に基づいて所定のアクセス権を設定するアクセス権設定手段と、設定されたアクセス権の範囲内でサーバコンピュータに対するアクセスを行うサーバアクセス手段と、を設けるようにしたものである。  
5

(6) 本発明の第6の態様は、ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、このクライアントコンピュータに接続して用いるために個々のユーザに発行された携帯可能情報処理装置と、を備えるコンピュータ  
10 システムにおいて、

各携帯可能情報処理装置に、それぞれクライアントコンピュータをネットワーク網の特定箇所に接続した場合に得られる特定のネットワーク環境を示す環境情報を記録しておき、

各クライアントコンピュータには、携帯可能情報処理装置を接続するための  
15 インターフェイス手段と、現在接続中の携帯可能情報処理装置から伝達されてきたアクセス権の範囲内でサーバコンピュータに対するアクセスを行うサーバアクセス手段と、を設け、

携帯可能情報処理装置には、現在接続中のクライアントコンピュータのネットワーク環境と自分自身に記録されている環境情報によって示されるネットワーク環境とを照合する環境照合手段と、この照合結果に基づいて所定のアクセス権を設定するアクセス権設定手段と、設定されたアクセス権を現在接続中のクライアントコンピュータに伝達するアクセス権伝達手段と、を設けるようにしたものである。  
20

(7) 本発明の第7の態様は、上述の第5または第6の態様に係るコンピュータシステムにおいて、  
25

アクセス権設定手段が、照合結果が一致した場合には第1のアクセス権を設

定し、照合結果が一致しなかった場合には第1のアクセス権よりも制限事項の多い第2のアクセス権を設定するようにしたものである。

(8) 本発明の第8の態様は、上述の第5～第7の態様に係るコンピュータシステムにおいて、

5 クライアントコンピュータに付与されたIPアドレス、クライアントコンピュータに設定されたデフォルトゲートウェイアドレス、クライアントコンピュータに設定されたプロキシサーバアドレス、もしくは、クライアントコンピュータが利用するDNSサーバによって照会可能なドメイン名を、当該クライアントコンピュータのネットワーク環境を示す環境情報として用いるようにした  
10 ものである。

(9) 本発明の第9の態様は、ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、このクライアントコンピュータに接続して用いるために個々のユーザに発行された携帯可能情報記録媒体と、を備えるコンピュータ  
15 システムにおいて、

各クライアントコンピュータに、それぞれ他のクライアントコンピュータと識別可能な固有の識別コードを記録しておき、

各携帯可能情報記録媒体に、それぞれ特定のクライアントコンピュータに記録されている特定の識別コードに対応する識別コードと、それぞれクライアントコンピュータをネットワーク網の特定箇所に接続した場合に得られる特定のネットワーク環境を示す環境情報と、を記録しておき、  
20

各クライアントコンピュータには、携帯可能情報記録媒体を接続するためのインターフェイス手段と、現在接続中の携帯可能情報記録媒体に記録されている識別コードと自分自身に記録されている識別コードとを照合する識別コード  
25 照合手段と、現在接続中の携帯可能情報記録媒体に記録されている環境情報によって示されるネットワーク環境と自分自身の現在のネットワーク環境とを照

合する環境照合手段と、これらの照合結果に基づいて所定のアクセス権を設定するアクセス権設定手段と、設定されたアクセス権の範囲内でサーバコンピュータに対するアクセスを行うサーバアクセス手段と、を設けるようにしたものである。

- 5 (10) 本発明の第10の態様は、ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、このクライアントコンピュータに接続して用いるために個々のユーザに発行された携帯可能情報処理装置と、を備えるコンピュータシステムにおいて、
  - 10 各クライアントコンピュータに、それぞれ他のクライアントコンピュータと識別可能な固有の識別コードを記録しておき、各携帯可能情報処理装置に、それぞれ特定のクライアントコンピュータに記録されている特定の識別コードに対応する識別コードと、それぞれクライアントコンピュータをネットワーク網の特定箇所に接続した場合に得られる特定の
  - 15 ネットワーク環境を示す環境情報と、を記録しておき、各クライアントコンピュータには、携帯可能情報処理装置を接続するためのインターフェイス手段と、現在接続中の携帯可能情報処理装置から伝達されてきたアクセス権の範囲内でサーバコンピュータに対するアクセスを行うサーバアクセス手段と、を設け、
- 20 携帯可能情報処理装置には、現在接続中のクライアントコンピュータに記録されている識別コードと自分自身に記録されている識別コードとを照合する識別コード照合手段と、現在接続中のクライアントコンピュータのネットワーク環境と自分自身に記録されている環境情報によって示されるネットワーク環境とを照合する環境照合手段と、これらの照合結果に基づいて所定のアクセス権を設定するアクセス権設定手段と、設定されたアクセス権を現在接続中のクライアントコンピュータに伝達するアクセス権伝達手段と、を設けるようにした
- 25

ものである。

(11) 本発明の第11の態様は、上述の第9または第10の態様に係るコンピュータシステムにおいて、

アクセス権設定手段が、識別コード照合手段による照合結果が一致した場合  
5 には第1のアクセス権を設定し、識別コード照合手段による照合結果は一致しないが環境照合手段による照合結果が一致した場合には第1のアクセス権よりも制限事項の多い第2のアクセス権を設定し、いずれの照合結果も一致しなかった場合には第2のアクセス権よりも更に制限事項の多い第3のアクセス権を設定するようにしたものである。

10 (12) 本発明の第12の態様は、上述の第9または第10の態様に係るコンピュータシステムにおいて、

アクセス権設定手段が、識別コード照合手段による照合結果と環境照合手段による照合結果との双方が一致した場合には第1のアクセス権を設定し、識別コード照合手段による照合結果は一致したが環境照合手段による照合結果は一致しない場合には第1のアクセス権よりも制限事項の多い第2のアクセス権を設定し、いずれの照合結果も一致しなかった場合には第2のアクセス権よりも更に制限事項の多い第3のアクセス権を設定するようにしたものである。

15 (13) 本発明の第13の態様は、ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、を備えるコンピュータシステムについて、個々のユーザがクライアントコンピュータを利用してサーバコンピュータへアクセスする際のアクセス権を設定する方法において、

20 個々のユーザに対して、クライアントコンピュータに接続して用いるための携帯可能情報処理装置を発行し、この携帯可能情報処理装置に、特定のクライアントコンピュータに記録されている識別コードであって当該特定のクライアントコンピュータを他のクライアントコンピュータと識別することが可能な固

有の識別コードに対応する識別コードを記録しておく準備段階と、

ユーザが、自分に対して発行された所定の携帯可能情報処理装置を所定のクライアントコンピュータに接続し、当該所定のクライアントコンピュータに対する利用開始手続を行ったときに、当該所定のクライアントコンピュータもし

5 くは当該所定の携帯可能情報処理装置によって、当該所定のクライアントコンピュータに記録されている識別コードと当該所定の携帯可能情報処理装置に記録されている識別コードとを照合させ、この照合結果に基づいて所定のアクセス権を設定させるアクセス権設定段階と、

を行い、アクセス権設定段階において、照合結果が一致しなかった場合には、

10 照合結果が一致した場合に比べて、制限事項の多いアクセス権の設定を行うようとしたものである。

(14) 本発明の第14の態様は、ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、を備えるコンピュータシステムについて、個々のユーザがクライアントコンピュータを利用してサーバコンピュータへアクセスする際のアクセス権を設定する方法において、

個々のユーザに対して、クライアントコンピュータに接続して用いるための携帯可能情報処理装置を発行し、この携帯可能情報処理装置に、クライアントコンピュータをネットワーク網の特定箇所に接続した場合に得られる特定のネットワーク環境を示す環境情報を記録しておく準備段階と、

ユーザが、自分に対して発行された所定の携帯可能情報処理装置を所定のクライアントコンピュータに接続し、当該所定のクライアントコンピュータに対する利用開始手続を行ったときに、当該所定のクライアントコンピュータもしくは当該所定の携帯可能情報処理装置によって、当該所定のクライアントコンピュータの現在のネットワーク環境と当該所定の携帯可能情報処理装置に記録されている環境情報によって示されるネットワーク環境とを照合させ、この照

合結果に基づいて所定のアクセス権を設定させるアクセス権設定段階と、  
を行い、アクセス権設定段階において、照合結果が一致しなかった場合には、  
照合結果が一致した場合に比べて、制限事項の多いアクセス権の設定を行うよ  
うにしたものである。

5 (15) 本発明の第15の態様は、ネットワーク網と、このネットワーク網に接  
続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクラ  
イアントコンピュータと、を備えるコンピュータシステムについて、個々のユ  
ーザがクライアントコンピュータを利用してサーバコンピュータへアクセスす  
る際のアクセス権を設定する方法において、

10 個々のユーザに対して、クライアントコンピュータに接続して用いるための  
携帯可能情報処理装置を発行し、この携帯可能情報処理装置に、特定のクライ  
アントコンピュータに記録されている識別コードであって当該特定のクライア  
ントコンピュータを他のクライアントコンピュータと識別することが可能な固  
有の識別コードに対応する識別コードと、クライアントコンピュータをネット  
15 ワーク網の特定箇所に接続した場合に得られる特定のネットワーク環境を示す  
環境情報と、を記録しておく準備段階と、  
ユーザが、自分に対して発行された所定の携帯可能情報処理装置を所定のク  
ライアントコンピュータに接続し、当該所定のクライアントコンピュータに対  
する利用開始手続を行ったときに、当該所定のクライアントコンピュータもし  
20 くは当該所定の携帯可能情報処理装置によって、当該所定のクライアントコン  
ピュータに記録されている識別コードと当該所定の携帯可能情報処理装置に記  
録されている識別コードとを照合させるとともに、当該所定のクライアントコ  
ンピュータの現在のネットワーク環境と当該所定の携帯可能情報処理装置に記  
録されている環境情報によって示されるネットワーク環境とを照合させ、これ  
25 らの照合結果に基づいて所定のアクセス権を設定させるアクセス権設定段階と、  
を行い、アクセス権設定段階において、識別コードの照合結果が一致した場

合には第1のアクセス権を設定し、識別コードの照合結果は一致しないがネットワーク環境の照合結果が一致した場合には第1のアクセス権よりも制限事項の多い第2のアクセス権を設定し、いずれの照合結果も一致しなかった場合には第2のアクセス権よりも更に制限事項の多い第3のアクセス権を設定するよう5 うにしたものである。

(16) 本発明の第16の態様は、ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、を備えるコンピュータシステムについて、個々のユーザがクライアントコンピュータを利用してサーバコンピュータへアクセスする際のアクセス権を設定する方法において、  
10

個々のユーザに対して、クライアントコンピュータに接続して用いるための携帯可能情報処理装置を発行し、この携帯可能情報処理装置に、特定のクライアントコンピュータに記録されている識別コードであって当該特定のクライアントコンピュータを他のクライアントコンピュータと識別することが可能な固有の識別コードに対応する識別コードと、クライアントコンピュータをネットワーク網の特定箇所に接続した場合に得られる特定のネットワーク環境を示す環境情報と、を記録しておく準備段階と、  
15

ユーザが、自分に対して発行された所定の携帯可能情報処理装置を所定のクライアントコンピュータに接続し、当該所定のクライアントコンピュータに対する利用開始手続を行ったときに、当該所定のクライアントコンピュータもしくは当該所定の携帯可能情報処理装置によって、当該所定のクライアントコンピュータに記録されている識別コードと当該所定の携帯可能情報処理装置に記録されている識別コードとを照合させるとともに、当該所定のクライアントコンピュータの現在のネットワーク環境と当該所定の携帯可能情報処理装置に記録されている環境情報によって示されるネットワーク環境とを照合させ、これらの照合結果に基づいて所定のアクセス権を設定させるアクセス権設定段階と、  
20  
25

を行い、アクセス権設定段階において、識別コードの照合結果とネットワーク環境の照合結果との双方が一致した場合には第1のアクセス権を設定し、識別コードの照合結果は一致したがネットワーク環境の照合結果は一致しない場合には第1のアクセス権よりも制限事項の多い第2のアクセス権を設定し、い  
5 ずれの照合結果も一致しなかった場合には第2のアクセス権よりも更に制限事項の多い第3のアクセス権を設定するようにしたものである。

(17) 本発明の第17の態様は、上述の第1～第12の態様に係るコンピュータシステムにおけるクライアントコンピュータとしてコンピュータを機能させるためのプログラムを用意し、当該プログラムをコンピュータ読み取り可能な  
10 記録媒体に記録して配付できるようにしたものである。

本発明に係るコンピュータシステムによれば、ユーザが利用しているクライアントコンピュータが、当該ユーザのために用意された特定のクライアントコンピュータであるか否か、あるいは、当該ユーザのために用意された特定のネットワーク環境にあるか否か、を認識することにより、アクセス権の設定を行うことができるので、個々のユーザに対して、状況に応じて異なるアクセス権を設定することが可能になる。  
15

### 図面の簡単な説明

図1は、ネットワーク網にサーバコンピュータとクライアントコンピュータとを接続して構成される一般的なコンピュータシステムを示すブロック図である。  
20

図2は、本発明の第1の実施形態を説明するためのブロック図であり、図1に示すコンピュータシステムの一部を示すものである。

図3は、図2に示す第1の実施形態を行うためのクライアントコンピュータの構成を示すブロック図である。  
25

図4は、図2に示す第1の実施形態において、携帯可能情報処理装置側で照

合処理およびアクセス権の設定処理を実行する変形例の構成を示すブロック図である。

図5は、本発明の第2の実施形態を説明するためのブロック図であり、図1に示すコンピュータシステムの一部を示すものである。

5 図6は、図5に示す第2の実施形態を行うためのクライアントコンピュータの構成を示すブロック図である。

図7は、図5に示す第2の実施形態において、携帯可能情報処理装置側で照合処理およびアクセス権の設定処理を実行する変形例の構成を示すブロック図である。

10 図8は、本発明の第3の実施形態を説明するためのブロック図であり、図1に示すコンピュータシステムの一部を示すものである。

図9は、図8に示す第3の実施形態を行うためのクライアントコンピュータの構成を示すブロック図である。

15 図10は、図8に示す3の実施形態において、携帯可能情報処理装置側で照合処理およびアクセス権の設定処理を実行する変形例の構成を示すブロック図である。

図11は、本発明の第3の実施形態におけるアクセス権の設定方法の一例を示す流れ図である。

20 図12は、本発明の第3の実施形態におけるアクセス権の設定方法の別な一例を示す流れ図である。

### 発明を実施するための最良の形態

以下、本発明を図示する実施形態に基づいて説明する。

<<< § 0. 本発明を導入する背景 >>>

25 はじめに、図1に示す例を参考にして、本発明を導入する背景を説明する。

図1は、ネットワーク網100に、2台のサーバコンピュータ110, 120

と、8台のクライアントコンピュータ11, 12, 13, 14, 21, 22, 23, 31とを接続して構成されるコンピュータシステムのモデルを示すブロック図である。一般的な企業で利用されているコンピュータシステムでは、より多数のサーバコンピュータや、より多数のクライアントコンピュータが用いられるのが普通であるが、ここでは便宜上、図示した単純なモデルについて説明を行うこととする。

ネットワーク網100は、通常、多数のルータやその間を接続する種々の回線によって構成される。一般に、ネットワークの形態としては、LAN, WAN, インターネットなど、様々な形態があるが、ネットワーク網100はどのような形態で構成してもかまわない。また、図では、ネットワーク網100と各クライアントコンピュータとの間を線で接続して示しているが、これらの間は必ずしも有線接続する必要はなく、無線LANを用いてもかまわない。

ここでは、説明の便宜上、このコンピュータシステムが、ある1つの企業で利用されているシステムであるものとし、クライアントコンピュータ11, 12, 13, 14は、この企業の人事部10に設置されており、クライアントコンピュータ21, 22, 23は、この企業の談話室20に設置されており、クライアントコンピュータ31は、この企業の社員寮30の一室に設置されているものとする。更に、人事部に所属する1人の社員をユーザ甲と呼ぶことにし、人事部10内のユーザ甲のデスクの上には、クライアントコンピュータ11が設置されているものとしよう。すなわち、ユーザ甲には、会社からクライアントコンピュータ11が支給されており、ユーザ甲は、自分のデスクに向かいながら、クライアントコンピュータ11を操作することにより、日常業務を遂行することになる。

一方、サーバコンピュータ110, 120には、この会社の業務上の様々なデータが蓄積されており、個々の社員は、必要に応じて、クライアントコンピュータからサーバコンピュータ110, 120へとアクセスし、必要なデータ

の読み出し、書き込み、改変などの処理を行うことになる。ここでは、説明の便宜上、サーバコンピュータ110には、全社員に対してアクセスを許可すべき汎用業務データが保存されており、サーバコンピュータ120には、特定の部署に所属する社員に対してのみアクセスさせるべき機密性の高い専用業務データが保存されているものとしよう。

もちろん、このようなコンピュータシステムを運用する上では、セキュリティの管理が重要である。従来の一般的なセキュリティ管理方法では、個々の社員に、その所属や職責に応じて、それぞれ固有のアクセス権を設定するような運用が行われる。上述の例の場合、人事部員であるユーザ甲には、たとえば、  
10 サーバコンピュータ110内の汎用業務データに対する読み出しを許可するアクセス権と、サーバコンピュータ120内的人事部専用業務データに対する読み出し／書き込みを許可するアクセス権とが設定される。

このように、ユーザごとのアクセス権管理を行うには、通常、個々のユーザにそれぞれ所定のアカウント（ユーザ名）とパスワードを付与し、個々のアカウントについてそれぞれ所定のアクセス権の設定を行っておき、特定のアカウントによるログイン手続があった場合には、パスワードの照合によりこのログイン手續が正規のものであることを確認した後、当該アカウントに設定されているアクセス権の範囲内でアクセスを許可する、という運用が行われる。たとえば、上述の例では、人事部員であるユーザ甲が、自分のデスクの上に設置されているクライアントコンピュータ11を起動して利用開始の手続を行うと、所定のアカウントとパスワードを入力する操作を要求されることになる。ここで入力したアカウントとパスワードが正規のものとして認証されると、以後は、予めユーザ甲に設定されているアクセス権の範囲内で、サーバコンピュータ110、120に対するアクセスが可能になる。

従来から行われている一般的なセキュリティ管理の手法は、上述の例のように、個々のユーザごとに特定のアクセス権を設定する、という基本方針に基づ

くものである。もちろん、個々の社員（ユーザ）が常に誠実に業務を遂行するであろうという前提に立てば、このような基本方針に基づくセキュリティ管理は非常に合理的である。しかしながら、多数の社員をかかえる企業では、社員の不正行為の可能性も考慮して、セキュリティ管理を行う必要がある。

5 たとえば、人事部員の暗黙の了解事項として、「個々の社員の給与明細を他の部署の者に見せてはならない」という規則があったとしよう。上述の例では、人事部員であるユーザ甲には、サーバコンピュータ 120 内の人事部専用業務データへのアクセス権が与えられているので、ユーザ甲は、自分のデスクの上のクライアントコンピュータ 11 の画面上に、個々の社員の給与明細を表示させ、その場で閲覧することは可能である。しかしながら、そのような状況下では、上記暗黙の了解事項を破るような行為が行われる可能性は低いであろう。少なくとも、クライアントコンピュータ 11 が設置された部屋には、人事部の他のスタッフも詰めており、上司による監督も行われているであろうから、他の部署の友人を自分のデスクの脇まで呼んできて、クライアントコンピュータ 11 上に表示させた給与明細を閲覧させる、というような行為を敢えて行うとは考えにくい。

ところが、このユーザ甲が、談話室 20 で友人と休憩している場合を考えると、状況は一転することが理解できよう。もし、ユーザ甲が、談話室 20 に設置されているクライアントコンピュータ 21 を利用してログインした場合にも、ユーザ甲としてのアクセス権がそのまま与えられるとすれば、談話室 20 に設置されているクライアントコンピュータ 21 の画面上にも、個々の社員の給与明細を表示させることが可能になる。談話室 20 では、上司の目も届かないでの、規則に反して、給与明細の情報を友人に閲覧させてしまう可能性は高い。更に、このユーザ甲が、社員寮 30 の自室に帰宅し、この自室に設置されたクライアントコンピュータ 31 を利用してログインした場合にも、ユーザ甲としてのアクセス権がそのまま与えられるとすれば、規則が破られる可能性は更に

高くなるであろう。

クライアントコンピュータの設置環境によって、規則違反が行われる可能性が高くなる例は、この他にも、枚挙にいとまがない。たとえば、「人事部員は、人事部長の許可がなければ、人事部専用業務データを外部の記録媒体に保存したりプリントアウトしてはならない」というような社内規則があったとしよう。この社内規則によれば、人事部員は、サーバコンピュータ120内の人事部専用業務データにアクセスすることは可能であるが、このデータを許可なくフロッピディスクやCD-Rに保存したり、プリントしたりすることは禁止される。したがって、人事部10に配置されたクライアントコンピュータ11～14を用いて、このような規則に反する行為が行われる可能性は低い。フロッピディスクに保存する行為やプリントアウトする行為は、上司や他のスタッフの目に触れやすいため、罪悪感により、違反行為は自粛されることになろう。しかしながら、談話室20に配置されたクライアントコンピュータ21～23や、社員寮30に配置されたクライアントコンピュータ31を用いた場合は事情が異なってくる。

また、機密性を重んじる部署では、当該部署の出入り口に監視カメラを設置したり、出入りの際に保守要員によるチェックを義務づけたりするケースもある。このような部署では、たとえ機密データをフロッピディスクやCD-Rに保存したり、プリントアウトしたりしても、それを部署外に持ち出すことが困難であるため、規則違反が行われる可能性は低い。ところが、社員寮30に設置されたクライアントコンピュータ31を利用した場合にも、同じアクセス権が与えられるとすると、当該部署の出入りを厳しくしても、セキュリティ上の意味はなくなってしまう。

もちろん、このようなセキュリティ上の問題を解決する手法として、通常、ファイアウォールを構築する方法が採られている。たとえば、図1に示す例の場合、ネットワーク網100内に多数のルータを組み込んで、個々のエリアご

とにファイアウォールを構築し、サーバコンピュータ120に対して、ノードN2やN3を経由したアクセスがあった場合には、これを拒絶する、というような運用を行えば、上述のような不正行為を防ぐことは可能である。しかしながら、そのためには、どこにどのようなファイアウォールを設置するか、とい  
5 うネットワーク網に関する複雑な設定が必要になる。本発明は、以下に述べる別なアプローチにより、このようなセキュリティ上の問題を解決するものである。

<<< § 1. 本発明の第1の実施形態 >>>

図2は、本発明の第1の実施形態を説明するためのブロック図であり、図1  
10 に示すコンピュータシステムの一部を示すものである。この第1の実施形態の基本概念は、個々のユーザについて、それぞれ本来のクライアントコンピュータを定めておき、各ユーザが、本来のクライアントコンピュータを用いてアクセスしてきた場合には、当該ユーザに設定されている本来のアクセス権によるアクセスを許可するが、それ以外のクライアントコンピュータを用いてアクセス  
15 してきた場合には、当該ユーザに設定されている本来のアクセス権よりも制限事項の多いアクセス権によるアクセスしか許可しないようにする、という運用にある。

いま、一例として、3人のユーザ甲、乙、丙がこのコンピュータシステムを利用する場合を考える。ここでは、ユーザ甲および乙は、いずれも人事部員であるものとし、ユーザ丙は、談話室を管理する庶務課員であるものとしよう。また、ユーザ甲には、本来のクライアントコンピュータとしてコンピュータ11が支給されており、ユーザ乙には、本来のクライアントコンピュータとしてコンピュータ12が支給されており、ユーザ丙には、本来のクライアントコンピュータとしてコンピュータ21が支給されているものとする。図1に示すように、ユーザ甲、乙に支給されたクライアントコンピュータ11、12は、人事部10の部屋に設置されており、ユーザ丙に支給されたクライアントコンピ

ユータ21は、談話室20に設置されている。

本発明に係るコンピュータシステムにおけるセキュリティ管理を行うためには、個々のユーザに対して、クライアントコンピュータに接続して用いるための携帯可能情報記録媒体が発行される。図2には、3人のユーザ甲、乙、丙に対して、それぞれ携帯可能情報記録媒体R11、R12、R21が発行された例が示されている。この携帯可能情報記録媒体R11、R12、R21は、各ユーザが容易に携帯することが可能であり、データを記録する機能をもった媒体であれば、どのようなものでもかまわない。ただ、実用上は、記録されたデータに対する十分なセキュリティを確保することが可能な媒体を用いるのが好ましい。具体的には、ICカードを携帯可能情報記録媒体として用いるのが最適である。ICカードは、携帯性に優れており、また、記録されているデータに対して十分なセキュリティを確保することが可能である。

なお、携帯可能情報記録媒体は、本発明に利用するための専用の媒体である必要はなく、他の用途と兼用することも可能である。たとえば、最近では、ICカードを利用した社員証などを各社員に発行する企業も増えてきているが、そのような場合は、社員証を携帯可能情報記録媒体として利用すれば足りる。ここでは、図2に示す携帯可能情報記録媒体R11、R12、R21が、それぞれユーザ甲、乙、丙に対して発行されたICカードからなる社員証であるものとして、以下の説明を行うこととする。

この第1の実施形態では、個々の携帯可能情報記録媒体R11、R12、R21に、それぞれ特定のクライアントコンピュータの識別コードを記録しておく。ここで、特定のクライアントコンピュータとは、各ユーザが利用すべき本来のコンピュータである。図2に示す例の場合、ユーザ甲に発行された携帯可能情報記録媒体R11（ユーザ甲の社員証として発行されたICカード）には、ユーザ甲が本来利用すべきクライアントコンピュータ11の識別コードID（11）が記録されている。同様に、ユーザ乙に発行された携帯可能情報記録

媒体R12（ユーザ乙の社員証として発行されたICカード）には、ユーザ乙が本来利用すべきクライアントコンピュータ12の識別コードID（12）が記録されており、ユーザ丙に発行された携帯可能情報記録媒体R21（ユーザ丙の社員証として発行されたICカード）には、ユーザ丙が本来利用すべきク

5 ライアントコンピュータ21の識別コードID（21）が記録されている。

クライアントコンピュータの識別コードとしては、当該クライアントコンピュータ内のいずれかの部分に記録されている識別コードであって、当該クライアントコンピュータを他のクライアントコンピュータと識別することが可能な固有の識別コードであれば、どのようなコードを用いてもかまわない。

10 たとえば、クライアントコンピュータに内蔵されているLAN通信回路に付与されたMACアドレス（Media Access Control Address）を、本発明における識別コードとして利用することができる。各クライアントコンピュータには、ネットワーク網100に接続するためのLAN通信回路が備わっている。現在、標準的に用いられているイーサネット用のLAN通信回路には、個々のメーカーが設定したユニークなMACアドレスが付与されている。しかも、このMACアドレスは、LAN通信回路内のICチップに記録されており、必要があれば、クライアントコンピュータのOSの機能を用いて読み出すことが可能である。したがって、このMACアドレスを識別コードとして用いれば、すべてのクライアントコンピュータを相互に識別することが可能になる。この場合、ユーザ甲の社員証として発行された携帯可能情報記録媒体R11には、クライアントコンピュータ11に内蔵されているLAN通信回路のMACアドレスを、

15 識別コードID（11）として記録しておけばよい。

20 もちろん、本発明における識別コードとして利用できるコードは、MACアドレスに限定されるものではなく、クライアントコンピュータの記憶装置に格納されている何らかの固有データであれば、MACアドレスと同様に識別コードとして利用することが可能である。たとえば、個々のクライアントコンピュ

25 ものとして利用することができる。たとえば、個々のクライアントコンピュ

ータごとに、それぞれユニークなシリアル番号が付与されており、このシリアル番号が、各クライアントコンピュータの内部に何らかの形で記録されていれば、当該シリアル番号を識別コードとして用いることも可能である。あるいは、意図的に、各クライアントコンピュータのハードディスクの特定領域に、それ  
5 ぞれユニークなシリアル番号を書き込んでおき、これを識別コードとして用いることも可能である。

また、各クライアントコンピュータの記憶装置に格納されているアプリケーションプログラムの構成を示す情報を、当該クライアントコンピュータを識別するための固有の識別コードとして用いることも可能である。通常、各クライ  
10 アントコンピュータには、その業務に応じてそれぞれ所定のアプリケーションプログラムがインストールされるので、特定のアプリケーションプログラムがインストールされているという事実を、識別コードとして利用することも可能である。もっとも、実際には、同一種類のアプリケーションプログラムがインストールされたコンピュータが多数存在することも少なくないので、その場合  
15 には、アプリケーションプログラムのインストール時に入力したシリアル番号を、アプリケーションプログラムの構成を示す情報とし、識別コードとして利用すればよい。すなわち、一般的なアプリケーションプログラムでは、インス  
トール時に所定のシリアル番号の入力が求められ、入力したシリアル暗号は、  
20 ハードディスク装置などに記録されることが多い。そこで、このアプリケーションプログラム用のシリアル番号を識別コードとして利用しても、個々のクライアントコンピュータを相互に区別することが可能である。

さて、図2に示す例のように、各ユーザ甲、乙、丙に対して発行した携帯可能情報記録媒体R11、R12、R21に、それぞれ特定のクライアントコンピュータの識別コードを記録する準備段階が完了したら、このコンピュータシステムの運用を開始することが可能になる。このコンピュータシステムでは、各ユーザは、それぞれ支給されたクライアントコンピュータを利用する際に、

社員証として発行されたＩＣカード、すなわち、携帯可能情報記録媒体を当該クライアントコンピュータに接続する作業を行うことが要求される。たとえば、ユーザ甲は、自分のデスクの上でクライアントコンピュータ11を利用する際に、社員証として発行されたＩＣカードである携帯可能情報記録媒体R11を、

5 クライアントコンピュータ11に接続して、所定の利用開始手続（一般に、ログイン手続あるいはログオン手続と呼ばれている手続）を行う必要がある。したがって、この実施形態では、各クライアントコンピュータには、ＩＣカード用のリーダライタ装置が装備されている。

本実施形態に係るコンピュータシステムにおけるセキュリティ管理の基本原

10 理は、ユーザが、自分に対して発行された所定の携帯可能情報記録媒体を所定のクライアントコンピュータに接続し、当該所定のクライアントコンピュータに対する利用開始手続を行ったときに、当該所定のクライアントコンピュータに記録されている識別コードと当該所定の携帯可能情報記録媒体に記録されている識別コードとを照合させ、この照合結果に基づいて所定のアクセス権を設定させる点にある。より具体的には、照合結果が一致しなかった場合には、照合結果が一致した場合に比べて、制限事項の多いアクセス権の設定を行うよう

15 にする。

たとえば、図2に示す例において、ユーザ甲が、自己の社員証として発行された携帯可能情報記録媒体R11を、人事部10に設置された本来使用すべき

20 クライアントコンピュータ11に接続して利用開始手続を行った場合、クライアントコンピュータ11に記録されている識別コードID(11)と携帯可能情報記録媒体R11に記録されている識別コードID(11)との照合作業が行われる。そして、この照合結果に基づいてアクセス権が設定される。この例の場合、照合結果は一致するので、クライアントコンピュータ11を利用した

25 ユーザ甲のアクセス行為に対しては、ユーザ甲に設定された本来のアクセス権が与えられることになる。たとえば、ユーザ甲には、サーバコンピュータ11

0内の汎用業務データに対する読み出しを許可するアクセス権と、サーバコンピュータ120内的人事部専用業務データに対する読み出し／書き込みを許可するアクセス権とが与えられる。

一方、ユーザ甲が、談話室20に設置されたクライアントコンピュータ21  
5 を利用したアクセスを行った場合を考えてみよう。この場合、ユーザ甲は、携帯可能情報記録媒体R11を、クライアントコンピュータ21に接続して利用開始手続を行うことになるが、クライアントコンピュータ21に記録されている識別コードID(21)と携帯可能情報記録媒体R11に記録されている識別コードID(11)とは一致しないので、この場合は、照合結果が一致した  
10 場合に比べて、制限事項の多いアクセス権の設定が行われる。たとえば、サーバコンピュータ110内の汎用業務データに対する読み出しは許可されるが、サーバコンピュータ120内的人事部専用業務データに対するアクセスは一切禁止されるようなアクセス権が与えられる。

このような運用を行えば、結局、各ユーザには、予め定められた本来のクライアントコンピュータを利用している場合には、本来のアクセス権が与えられることになるが、それ以外のクライアントコンピュータを利用している場合には、ユーザのアクセス権は制限されることになる。上述の例の場合、人事部員であるユーザ甲は、人事部10に設置されたクライアントコンピュータ11で作業する限りは、人事部員に与えられる本来のアクセス権をもって各サーバコンピュータへのアクセスが可能になるが、談話室20や社員寮30に設置されたクライアントコンピュータを利用した場合は、本来のアクセス権を取得することはできない。したがって、§0で述べたようなセキュリティ上の問題を解決することができる。

ところで、識別コードの照合処理や、照合結果に応じたアクセス権の設定処理を行うためには、クライアントコンピュータ内にそれなりの構成要素を用意しておく必要がある。図3は、この第1の実施形態を行うためのクライアント

コンピュータ11の構成を示すブロック図である。図示のとおり、クライアントコンピュータ11には、サーバアクセス手段11A、アクセス権設定手段11B、識別コード照合手段11C、インターフェイス手段11Dが設けられている。もちろん、クライアントコンピュータ11には、この他にも、クライアントコンピュータとしての機能を果たすための種々の構成要素（たとえば、OSプログラムやアプリケーションプログラムを実行するためのCPU、メモリ、ハードディスクや、入出力装置など）が備わっているが、ここでは説明は省略する。

前述したとおり、このクライアントコンピュータ11には、他のクライアントコンピュータと識別可能な固有の識別コードID(11)が記録されている。たとえば、MACアドレスを識別コードID(11)として利用するようすれば、識別コードID(11)はもともとクライアントコンピュータ11内に組み込まれていることになるので、識別コードをクライアントコンピュータ11に書き込むような作業は一切不要である。一方、携帯可能情報記録媒体R11にも、識別コードID(11)が記録されている。こちらの方は、このコンピュータシステムの管理者による書き込み作業が必要になる。ここに示す例では、携帯可能情報記録媒体R11は、ユーザ甲の社員証として発行されたICカードであるため、その中には、識別コードID(11)以外のデータも多数記録されているが、ここではそれらの説明は省略する。

ここで、インターフェイス手段11Dは、携帯可能情報記録媒体R11を接続するための構成要素であり、この例の場合、ICカード用のリーダライタ装置によって構成されている。ユーザは、このクライアントコンピュータ11に対する利用開始手続を行う際に、ICカードとしての携帯可能情報記録媒体R11を、リーダライタ装置としてのインターフェイス手段11Dに装填することにより、両者を接続状態にすることができる。また、利用を終了する際には、このICカードを、リーダライタ装置から引き抜くことにより、両者を分離す

ることができる。

識別コード照合手段 11C は、現在接続中の携帯可能情報記録媒体に記録されている識別コードと自分自身に記録されている識別コードとを照合する機能を有する構成要素であり、アクセス権設定手段 11B は、この照合結果に基づいて所定のアクセス権を設定する機能を有する構成要素である。アクセス権設定手段 11B は、照合結果が一致した場合には第 1 のアクセス権を設定し、照合結果が一致しなかった場合にはこの第 1 のアクセス権よりも制限事項の多い第 2 のアクセス権を設定することになる。サーバアクセス手段 11A は、設定されたアクセス権の範囲内で、サーバコンピュータ 110, 120 に対するアクセスを行う構成要素である。

図示の例の場合、ユーザ甲が自己の社員証である携帯可能情報記録媒体 R11 を用いて、クライアントコンピュータ 11 への利用開始手続を行っているので、識別コード照合手段 11C による照合結果は一致する。すなわち、識別コード照合手段 11C は、インターフェイス手段 11D を介して読み出した携帯可能情報記録媒体 R11 内の識別コード ID (11) と、クライアントコンピュータ 11 内に記録されていた識別コード ID (11) とを比較照合する処理を行うことになるので、この例の場合は、両者が一致する結果が得られるので、アクセス権設定手段 11B は、第 1 のアクセス権を設定する。

もし、談話室 20 に設置されたクライアントコンピュータ 21 に対して、同様の利用開始手続を行ったとすると、携帯可能情報記録媒体 R11 内の識別コード ID (11) と、クライアントコンピュータ 21 内に記録されていた識別コード ID (21) とは一致しないので、クライアントコンピュータ 21 内の識別コード照合手段 21C は不一致の結果を示し、アクセス権設定手段 21B は、第 2 のアクセス権を設定することになる。

上述した例では、第 1 のアクセス権としては、サーバコンピュータ 110 内の汎用業務データに対する読み出しを許可するとともに、サーバコンピュータ 1

20 内の人事部専用業務データに対する読み出し／書き込みを許可する権利を設定し、第2のアクセス権としては、サーバコンピュータ110内の汎用業務データに対する読み出しを許可するが、サーバコンピュータ120内のデータに対するアクセスは一切禁止する権利を設定することになる。

- 5 もっとも、このようなアクセス許否の具体的な内容設定は、必ずしもクライアントコンピュータ内のアクセス権設定手段によって行う必要はない。実用上は、むしろ、アクセス権設定手段においては、第1のアクセス権か第2のアクセス権かのいずれかを設定するだけにしておき、細かなアクセス許否の設定は、サーバコンピュータ側で行うようにするのが好ましい。たとえば、サーバコンピュータ120内的人事部専用業務データについては、第1のアクセス権をもったユーザ甲からのアクセスがあった場合には、読み出し／書き込みを許可するが、第2のアクセス権をもったユーザ甲からのアクセスがあった場合には、一切のアクセスを拒絶する、というような設定を行っておけばよい。この場合、ユーザ甲からのアクセスであることの認証は、従来どおり、ユーザ甲に与えた
- 10 アカウント名とパスワードの照合により行うようにすればよい。
- 15

なお、識別コードの照合処理や、照合結果に応じたアクセス権の設定処理は、必ずしもクライアントコンピュータ側で行う必要はない。すなわち、携帯可能情報記録媒体が情報処理機能を有している場合には、携帯可能情報記録媒体側でこれらの処理を実行させることも可能である。現在、社員証などに利用されているICカードには、単なる情報記録媒体としての機能だけでなく、CPUを内蔵した情報処理装置としての機能も備わっている。このような情報処理機能を備えた携帯可能情報記録媒体（以下、携帯可能情報処理装置という）を用いれば、識別コードの照合処理およびアクセス権の設定処理を、携帯可能情報処理装置側で行うことが可能になる。

- 20
- 25 図4は、この第1の実施形態において、携帯可能情報処理装置側で照合処理およびアクセス権の設定処理を実行する変形例の構成を示すブロック図である。

図示のとおり、クライアントコンピュータ11内に、固有の識別コードID(11)が記録されており、携帯可能情報処理装置P11内に、このクライアントコンピュータ11に記録されている識別コードに対応する識別コードID(11)が記録されている点は、図3に示す例と全く同様である。ただ、クライアントコンピュータ11には、現在接続中の携帯可能情報処理装置から伝達されてきたアクセス権の範囲内でサーバコンピュータに対するアクセスを行うサーバアクセス手段11Aと、携帯可能情報処理装置を接続するためのインターフェイス手段11Dと、が備わっているものの、識別コード照合手段およびアクセス権設定手段は備わっていない。

一方、携帯可能情報処理装置P11は、上述したように、情報処理機能をもったICカードであり、図示のとおり、識別コード照合手段11E、アクセス権設定手段11F、アクセス権伝達手段11Gを備えている。識別コード照合手段11Eは、現在接続中のクライアントコンピュータに記録されている識別コードと自分自身に記録されている識別コードとを照合する構成要素であり、アクセス権設定手段11Fは、この照合結果に基づいて所定のアクセス権を設定する構成要素であり、アクセス権伝達手段11Gは、設定されたアクセス権を現在接続中のクライアントコンピュータに伝達する構成要素である。

図示のように、ユーザ甲が自己の社員証である携帯可能情報処理装置P11(情報処理機能をもったICカード)を用いて、クライアントコンピュータ11への利用開始手続を行うと、識別コード照合手段11Eは、インターフェイス手段11Dを介して読み出したクライアントコンピュータ11内の識別コードID(11)と、携帯可能情報処理装置P11内に記録されていた識別コードID(11)とを比較照合する処理を行うことになる。この例の場合は、両者が一致する結果が得られるので、アクセス権設定手段11Fは、第1のアクセス権を設定し、設定したアクセス権は、インターフェイス手段11Dを介して、サーバアクセス手段11Aへと伝えられる。その結果、サーバアクセス手

段 1 1 A は、第 1 のアクセス権に基づいてサーバコンピュータへのアクセスを行うことになる。

もちろん、談話室 2 0 に設置されたクライアントコンピュータ 2 1 に対して、同様の利用開始手続を行ったとすると、携帯可能情報処理装置 P 1 1 内の識別コード ID (1 1) と、クライアントコンピュータ 2 1 内に記録されていた識別コード ID (2 1) とは一致しないので、識別コード照合手段 1 1 E では、不一致の照合結果が得られることになり、アクセス権設定手段 1 1 F は、第 2 のアクセス権を設定する。その結果、サーバアクセス手段 1 1 A は、第 2 のアクセス権に基づいてサーバコンピュータへのアクセスを行うことになる。

10 <<< § 2. 本発明の第 2 の実施形態 >>>

図 5 は、本発明の第 2 の実施形態を説明するためのブロック図であり、図 1 に示すコンピュータシステムの一部を示すものである。この第 2 の実施形態の基本概念は、個々のユーザについて、それぞれ本来のクライアントコンピュータを定める代わりに、本来のネットワーク環境を定めておき、各ユーザが、本来のネットワーク環境に接続されたクライアントコンピュータを用いてアクセスしてきた場合には、当該ユーザに設定されている本来のアクセス権によるアクセスを許可するが、それ以外のネットワーク環境に接続されたクライアントコンピュータを用いてアクセスしてきた場合には、当該ユーザに設定されている本来のアクセス権よりも制限事項の多いアクセス権によるアクセスしか許可しないようとする、という運用にある。

すなわち、上述した第 1 の実施形態では、各ユーザが予め定められた特定のクライアントコンピュータからアクセスしているか否かに応じて異なるアクセス権の設定を行っていたのに対して、この第 2 の実施形態では、各ユーザが予め定められた特定のネットワーク環境からアクセスしているか否かに応じて異なるアクセス権の設定を行うことになる。ここで、ネットワーク環境とは、クライアントコンピュータをネットワーク網 1 0 0 の特定箇所に接続した場合に

得られる環境を意味するものであり、たとえば、図1に示す例において、ネットワーク網100のノードN1を経由してサーバコンピュータ110, 120へのアクセスを行うクライアントコンピュータ11～14と、ノードN2を経由してサーバコンピュータ110, 120へのアクセスを行うクライアントコンピュータ21～23と、ノードN3を経由してサーバコンピュータ110, 120へのアクセスを行うクライアントコンピュータ31とは、いずれもネットワーク環境が異なるコンピュータということになる。

もっとも、ネットワーク環境は、あくまでもネットワーク網100に対する接続環境を示すものであり、個々のクライアントコンピュータと直接関連するものではない。たとえば、図1に示す談話室20に設置されているクライアントコンピュータ23を、談話室20内のLANから取り外し、人事部10へと移動し、人事部10のLANに接続したとすると、同一のクライアントコンピュータ23でありながら、ネットワーク環境は変わってしまうことになる。逆に、人事部10に設置されているクライアントコンピュータ11が故障したため、同一の設置場所において、これを新品のクライアントコンピュータ15に取り換えた場合、クライアントコンピュータ自身は異なるものになるが、ネットワーク環境に変化はない。

前述した第1の実施形態の場合、個々のクライアントコンピュータに固有のMACアドレスなどを識別コードとして用いると、コンピュータを新品に入れ替えたような場合、識別コードも変わってしまうことになる。その場合、携帯可能情報記録媒体に記録した識別コードも新たなものに書き換える作業が必要になる。ここで述べる第2の実施形態の場合、クライアントコンピュータ自身の同一性ではなく、ネットワーク環境の同一性を判断して、アクセス権の設定が行われるため、ネットワーク環境の同一性が確保されている限り、コンピュータを入れ替えたとしても、携帯可能情報記録媒体への記録内容を書き換えるような作業は必要ない。

図5には、3人のユーザ甲、乙、丙に対して、この第2の実施形態に基づいて、それぞれ携帯可能情報記録媒体R11、R12、R21が発行された例が示されている。前述したとおり、この携帯可能情報記録媒体R11、R12、R21は、それぞれユーザ甲、乙、丙に対して発行されたICカードからなる  
5 社員証である。

この第2の実施形態では、個々の携帯可能情報記録媒体R11、R12、R21に、クライアントコンピュータをネットワーク網100の特定箇所に接続した場合に得られる特定のネットワーク環境を示す環境情報を記録しておくことになる。ここで記録される環境情報は、各ユーザが利用すべき本来のネットワーク環境を示すものになる。図5に示す例の場合、ユーザ甲に発行された携帯可能情報記録媒体R11（ユーザ甲の社員証として発行されたICカード）には、ユーザ甲が本来利用すべきネットワーク環境を示す環境情報ENV（11）が記録されている。具体的には、ユーザ甲が自分のデスクで利用しているクライアントコンピュータ11についてのネットワーク環境を示す環境情報ENV（11）が、そのまま携帯可能情報記録媒体R11内に記録されることになる。同様に、ユーザ乙に発行された携帯可能情報記録媒体R12（ユーザ乙の社員証として発行されたICカード）には、ユーザ乙が本来利用すべきネットワーク環境を示す環境情報ENV（12）が記録されており、ユーザ丙に発行された携帯可能情報記録媒体R21（ユーザ丙の社員証として発行されたICカード）には、ユーザ丙が本来利用すべきネットワーク環境を示す環境情報ENV（21）が記録されている。  
10  
15  
20

ネットワーク環境を示す環境情報としては、クライアントコンピュータをネットワーク網100の特定箇所に接続した場合に得られる特定のネットワーク環境を示す情報であれば、どのような情報を用いてもかまわないが、以下に、  
25 環境情報として利用できる具体的な情報の例をいくつか挙しておく。

たとえば、クライアントコンピュータに付与されたIPアドレスを環境情報

として利用することが可能である。通常、企業のコンピュータシステムを構成するコンピュータには、DHCP (Dynamic Host Configuration Protocol) を利用して、所定のIPアドレスが自動的に割り当てられる。このとき、各ネットワークのエリアごとに、それぞれ所定のアドレス範囲を定める運用が行われている場合には、ネットワーク網100に対する接続箇所に応じて、割り当てられるアドレス範囲が異なることになる。たとえば、図1に示す例において、ネットワーク網100のノードN1, N2, N3にそれぞれルータが設けられており、ノードN1に接続されている人事部10のクライアントコンピュータ11, 12, 13, 14に対しては、第1のアドレス範囲に属するIPアドレスが割り当てられ、ノードN2に接続されている談話室20のクライアントコンピュータ21, 22, 23に対しては、第2のアドレス範囲に属するIPアドレスが割り当てられ、ノードN3に接続されている社員寮30のクライアントコンピュータ31に対しては、第3のアドレス範囲に属するIPアドレスが割り当てられている場合、クライアントコンピュータに現時点で割り当てられているIPアドレスが、どのアドレス範囲に属するかを確認することにより、当該クライアントコンピュータのネットワーク環境を認識することができる。

たとえば、あるクライアントコンピュータに割り当てられたIPアドレスが第1のアドレス範囲に属するものであったとすると、当該クライアントコンピュータは、ノードN1に接続されている人事部10のコンピュータであることが認識できる。IPv4の場合、IPアドレスは32ビットの数字により表現されるが、たとえば、同一ノードに接続されるクライアントコンピュータには、上位24ビットが同一で下位8ビットのみが異なるIPアドレスを付与するような規則でIPアドレスの決定が行われるような場合なら、IPアドレスの上位24ビットをそのままネットワーク環境を示す環境情報として利用することができる。図1に示す例の場合、たとえば、人事部10に所属するクライアントコンピュータ11, 12, 13, 14の各IPアドレスの上位24ビットは

同一になるので、これをそのまま環境情報として利用することができる。

また、クライアントコンピュータに設定されたデフォルトゲートウェイアドレ<sup>5</sup>スを、ネットワーク環境を示す環境情報として利用することもできる。たとえば、図1に示す例において、ノードN1, N2, N3にそれぞれルータが設

置されていたとすると、各クライアントコンピュータについて設定されるデフォルトゲートウェイアドレスは、それぞれのノードに設置されたルータのIPアドレスになる。たとえば、人事部10のクライアントコンピュータ11, 12, 13, 14には、ノードN1に設置されたルータのIPアドレスが、共通のデフォルトゲートウェイアドレスとして設定される。これに対して、談話室20のクライアントコンピュータ21, 22, 23には、ノードN2に設置されたルータのIPアドレスが、共通のデフォルトゲートウェイアドレスとして設定される。したがって、これらのデフォルトゲートウェイアドレスを、そのままネットワーク環境を示す環境情報として利用することができる。

ノードN1, N2, N3に、ルータではなく、プロキシサーバが設置されている場合には、クライアントコンピュータに設定されたプロキシサーバアドレスを、ネットワーク環境を示す環境情報として利用することもできる。人事部10のクライアントコンピュータ11, 12, 13, 14には、共通のプロキシサーバアドレスが設定されることになるが、談話室20のクライアントコンピュータ21, 22, 23には、それとは別な共通のプロキシサーバアドレスが設定されることになる。

この他、クライアントコンピュータが利用するDNSサーバによって照会可能なドメイン名を、当該クライアントコンピュータのネットワーク環境を示す環境情報として用いることも可能である。DNSサーバは、ドメイン名とIPアドレスとを相互に変換する変換テーブル機能をもったサーバコンピュータである。図1に示す例において、もし、人事部10に設置された各クライアントコンピュータが参照するDNSサーバと、談話室20に設置された各クライア

ントコンピュータが参照するDNSサーバとが異なっており、それぞれの変換テーブルの内容が異なっている場合には、この差異を利用して、いずれのDNSサーバを参照するクライアントコンピュータであるかを認識することが可能になる。

- 5 たとえば、人事部10に設置された各クライアントコンピュータが参照するDNSサーバには、「Melon」なるドメイン名をIPアドレスに変換するテーブルが用意されているが、談話室20に設置された各クライアントコンピュータが参照するDNSサーバには、「Melon」なるドメイン名を変換するテーブルが用意されていなかったとすれば、あるクライアントコンピュータから、「Melon」なるドメイン名を検索する操作を行い、検索が行えた場合には、当該クライアントコンピュータは、人事部10に設置されたクライアントコンピュータであると認識することができる。

- 10 以上述べたとおり、クライアントコンピュータをネットワーク網100の特定箇所に接続した場合に得られる特定のネットワーク環境を示す様々な情報を、
- 15 この第2の実施形態における環境情報として利用することが可能である。ここでは、図5に示す例のように、各ユーザ甲、乙、丙に対して発行した携帯可能情報記録媒体R11、R12、R21に、それぞれ特定の環境情報を記録する準備段階が完了したものとしよう。たとえば、ユーザ甲の社員証である携帯可能情報記録媒体R11内に記録されている環境情報ENV(11)は、ユーザ甲が利用する本来のネットワーク環境を示す情報であり、具体的には、クライアントコンピュータ11に付与されたIPアドレスの上位24ビットであったり、ノードN1に設置されているルータのIPアドレス（デフォルトゲートウェイアドレス）であったり、ノードN1に設置されているプロキシサーバのアドレスであったりする。

- 20 25 図5に示す例の場合、クライアントコンピュータ11のネットワーク環境とクライアントコンピュータ12のネットワーク環境とは同一であり、環境情報

ENV(11)と環境情報ENV(12)とは同一になる。ただし、クライアントコンピュータ21のネットワーク環境は異なるものになるので、環境情報ENV(21)も異なるものになる。

本実施形態に係るコンピュータシステムにおけるセキュリティ管理の基本原理は、ユーザが、自分に対して発行された所定の携帯可能情報記録媒体を所定のクライアントコンピュータに接続し、当該所定のクライアントコンピュータに対する利用開始手続を行ったときに、当該所定のクライアントコンピュータの現時点でのネットワーク環境と、当該所定の携帯可能情報記録媒体に記録されている環境情報によって示されるネットワーク環境とを照合させ、この照合結果に基づいて所定のアクセス権を設定させる点にある。より具体的には、照合結果が一致しなかった場合には、照合結果が一致した場合に比べて、制限事項の多いアクセス権の設定を行うようとする。この点は、前掲の第1の実施形態と同様である。

たとえば、図5に示す例において、ユーザ甲が、自己の社員証として発行された携帯可能情報記録媒体R11を、人事部10のクライアントコンピュータ11に接続して利用開始手続を行った場合、クライアントコンピュータ11のネットワーク環境を示す環境情報ENV(11)と携帯可能情報記録媒体R11に記録されている環境情報ENV(11)との照合作業が行われる。そして、この照合結果に基づいてアクセス権が設定される。この例の場合、照合結果は一致するので、クライアントコンピュータ11を利用したユーザ甲のアクセス行為に対しては、ユーザ甲に設定された本来のアクセス権が与えられることになる。たとえば、ユーザ甲には、サーバコンピュータ110内の汎用業務データに対する読み出しを許可するアクセス権と、サーバコンピュータ120内の人事部専用業務データに対する読み出し／書き込みを許可するアクセス権とが与えられる。

ところで、図5に示す例において、クライアントコンピュータ11のネット

ワーク環境とクライアントコンピュータ12のネットワーク環境とは同一であるので、環境情報ENV(11)と環境情報ENV(12)とは同一になる。したがって、ユーザ甲が、クライアントコンピュータ12を利用した場合も、上述の場合と全く同じアクセス権が与えられることになる。もちろん、クライアントコンピュータ11を、新たなクライアントコンピュータ15に交換し、この新たなクライアントコンピュータ15を利用した場合も、同じアクセス権が与えられることになる。このように、ここで述べる第2の実施形態では、前述した第1の実施形態よりも自由度の高い運用が可能になる。

一方、ユーザ甲が、談話室20に設置されたクライアントコンピュータ21を利用したアクセスを行った場合は、事情が変わってくる。この場合、ユーザ甲は、携帯可能情報記録媒体R11を、クライアントコンピュータ21に接続して利用開始手続を行うことになるが、クライアントコンピュータ21のネットワーク環境を示す環境情報ENV(21)と携帯可能情報記録媒体R11に記録されている環境情報ENV(11)とは一致しないので、この場合は、照合結果が一致した場合に比べて、制限事項の多いアクセス権の設定が行われる。たとえば、サーバコンピュータ110内の汎用業務データに対する読み出しは許可されるが、サーバコンピュータ120内的人事部専用業務データに対するアクセスは一切禁止されるようなアクセス権が与えられる。

このような運用を行えば、結局、各ユーザには、予め定められた本来のネットワーク環境からのアクセスを行う限り、本来のアクセス権が与えられることになるが、それ以外のネットワーク環境からアクセスした場合、ユーザのアクセス権は制限されることになる。上述の例の場合、人事部員であるユーザ甲は、人事部10に設置されたクライアントコンピュータ11～14を用いてアクセスする限りは、人事部員に与えられる本来のアクセス権をもって各サーバコンピュータへのアクセスが可能になるが、談話室20や社員寮30に設置されたクライアントコンピュータを利用した場合は、本来のアクセス権を取得するこ

とはできない。したがって、§0で述べたようなセキュリティ上の問題を解決することができる。

この第2の実施形態においても、環境情報の照合処理や、照合結果に応じたアクセス権の設定処理を行うために、クライアントコンピュータ内にそれなりの構成要素を用意しておく必要がある。図6は、この第2の実施形態を行うためのクライアントコンピュータ11の構成を示すブロック図である。図示のとおり、クライアントコンピュータ11には、サーバアクセス手段11A、アクセス権設定手段11B、環境照合手段11H、インターフェイス手段11Dが設けられている。もちろん、クライアントコンピュータ11には、この他にも、クライアントコンピュータとしての機能を果たすための種々の構成要素（たとえば、OSプログラムやアプリケーションプログラムを実行するためのCPU、メモリ、ハードディスクや、入出力装置など）が備わっているが、ここでは説明は省略する。

このクライアントコンピュータ11は、特定のネットワーク環境下でネットワーク網100に接続されており、当該特定のネットワーク環境は、所定の環境情報ENV(11)によって示すことができる。環境情報ENV(11)としては、クライアントコンピュータ11に設定されたIPアドレス、デフォルトゲートウェイアドレス、プロキシサーバアドレスなどを用いることができる点は、既に述べたとおりである。

インターフェイス手段11Dは、図3に示す実施形態の場合と同様に、携帯可能情報記録媒体R11を接続するための構成要素であり、ICカード用のリーダライタ装置によって構成されている。ユーザは、このクライアントコンピュータ11に対する利用開始手続を行う際に、ICカードとしての携帯可能情報記録媒体R11を、リーダライタ装置としてのインターフェイス手段11Dに装填することにより、両者を接続状態にすることができる。また、利用を終了する際には、このICカードを、リーダライタ装置から引き抜くことにより、

両者を分離することができる。

環境照合手段 1 1 H は、現在接続中の携帯可能情報記録媒体に記録されている環境情報とクライアントコンピュータ 1 1 の現在のネットワーク環境を示す環境情報とを照合する機能を有する構成要素であり、アクセス権設定手段 1 1  
5 B は、この照合結果に基づいて所定のアクセス権を設定する機能を有する構成要素である。アクセス権設定手段 1 1 B は、照合結果が一致した場合には第 1 のアクセス権を設定し、照合結果が一致しなかった場合にはこの第 1 のアクセス権よりも制限事項の多い第 2 のアクセス権を設定することになる。サーバアクセス手段 1 1 A は、設定されたアクセス権の範囲内で、サーバコンピュータ  
10 1 1 0, 1 2 0 に対するアクセスを行う構成要素である。

図 6 に示す例の場合、ユーザ甲が自己の社員証である携帯可能情報記録媒体 R 1 1 を用いて、クライアントコンピュータ 1 1 への利用開始手続を行っているので、環境照合手段 1 1 H による照合結果は一致する。すなわち、環境照合手段 1 1 H は、インターフェイス手段 1 1 D を介して読み出した携帯可能情報記録媒体 R 1 1 内の環境情報 ENV (1 1) と、クライアントコンピュータ 1 1 の現時点のネットワーク環境を示す環境情報 ENV (1 1) とを比較照合する処理を行うことになるので、この例の場合は、両者が一致する結果が得られ、  
15 アクセス権設定手段 1 1 B は、第 1 のアクセス権を設定する。

もし、談話室 2 0 に設置されたクライアントコンピュータ 2 1 に対して、同様の利用開始手続を行ったとすると、携帯可能情報記録媒体 R 1 1 内の環境情報 ENV (1 1) と、クライアントコンピュータ 2 1 のネットワーク環境を示す環境情報 ENV (2 1) とは一致しないので、クライアントコンピュータ 2 1 内の環境照合手段 2 1 H は不一致の結果を示し、アクセス権設定手段 2 1 B は、第 2 のアクセス権を設定することになる。第 1 のアクセス権によるアクセスと、第 2 のアクセス権によるアクセスとの相違は、既に、§ 1 で述べたとおりである。

図7は、この第2の実施形態において、携帯可能情報処理装置側で照合処理およびアクセス権の設定処理を実行する変形例の構成を示すブロック図である。図示のとおり、クライアントコンピュータ11には、現在接続中の携帯可能情報処理装置から伝達されてきたアクセス権の範囲内でサーバコンピュータに対するアクセスを行うサーバアクセス手段11Aと、携帯可能情報処理装置を接続するためのインターフェイス手段11Dと、が備わっているものの、環境照合手段およびアクセス権設定手段は備わっていない。

一方、携帯可能情報処理装置P11は、情報処理機能をもったICカードであり、図示のとおり、環境照合手段11I、アクセス権設定手段11F、アクセス権伝達手段11Gを備えている。環境照合手段11Iは、現在接続中のクライアントコンピュータのネットワーク環境を示す環境情報と自分自身に記録されている環境情報とを照合する構成要素であり、アクセス権設定手段11Fは、この照合結果に基づいて所定のアクセス権を設定する構成要素であり、アクセス権伝達手段11Gは、設定されたアクセス権を現在接続中のクライアントコンピュータに伝達する構成要素である。

図示のように、ユーザ甲が自己の社員証である携帯可能情報処理装置P11（情報処理機能をもったICカード）を用いて、クライアントコンピュータ11への利用開始手続を行うと、環境照合手段11Iは、インターフェイス手段11Dを介して読み出したクライアントコンピュータ11のネットワーク環境を示す環境情報ENV（11）と、携帯可能情報処理装置P11内に記録されていた環境情報ENV（11）とを比較照合する処理を行うことになる。この例の場合は、両者が一致する結果が得られるので、アクセス権設定手段11Fは、第1のアクセス権を設定し、設定したアクセス権は、インターフェイス手段11Dを介して、サーバアクセス手段11Aへと伝えられる。その結果、サーバアクセス手段11Aは、第1のアクセス権に基づいてサーバコンピュータへのアクセスを行うことになる。

もちろん、談話室 20 に設置されたクライアントコンピュータ 21 に対して、同様の利用開始手続を行ったとすると、携帯可能情報処理装置 P11 内の環境情報 ENV(11) と、クライアントコンピュータ 21 のネットワーク環境を示す環境情報 ENV(21) とは一致しないので、環境照合手段 11I では、

5 不一致の照合結果が得られることになり、アクセス権設定手段 11F は、第 2 のアクセス権を設定する。その結果、サーバアクセス手段 11A は、第 2 のアクセス権に基づいてサーバコンピュータへのアクセスを行うことになる。

<<< § 3. 本発明の第 3 の実施形態 >>>

ここで述べる第 3 の実施形態は、§ 1 で述べた第 1 の実施形態と § 2 で述べた第 2 の実施形態との組み合わせに相当するものである。すなわち、第 1 の実施形態の特徴は、個々のユーザに対して、それぞれ本来利用すべき特定のクライアントコンピュータを設定しておき、当該クライアントコンピュータからのアクセスか否かによって、アクセス権の設定を変えることにあり、第 2 の実施形態の特徴は、個々のユーザに対して、それぞれ本来利用すべき特定のネットワーク環境を設定しておき、当該ネットワーク環境からのアクセスか否かによって、アクセス権の設定を変えることがある。ここで述べる第 3 の実施形態の特徴は、個々のユーザに対して、それぞれ本来利用すべき特定のクライアントコンピュータと、本来利用すべき特定のネットワーク環境とを設定しておき、当該クライアントコンピュータからのアクセスか否かという点と、当該ネットワーク環境からのアクセスか否かという点とを考慮して、アクセス権の設定を変えることにある。

したがって、この第 3 の実施形態では、個々のユーザに対して発行した携帯可能情報記録媒体に特定の識別コードと、特定のネットワーク環境を示す環境情報と、を記録しておくことになる。ユーザが、クライアントコンピュータに対して利用開始手続を行うと、当該クライアントコンピュータに記録されている識別コードと携帯可能情報記録媒体に記録されている識別コードとの照合処

理と、当該クライアントコンピュータの現在のネットワーク環境と携帯可能情報記録媒体に記録されている環境情報によって示されるネットワーク環境との照合処理が行われ、これらの照合結果に基づいて所定のアクセス権が設定されることになる。

5 図8は、本発明の第3の実施形態を説明するためのブロック図であり、図1に示すコンピュータシステムの一部を示すものである。ここでも、3人のユーザ甲、乙、丙に対して、それぞれ携帯可能情報記録媒体R11、R12、R21が発行された例が示されている。個々の携帯可能情報記録媒体R11、R12、R21には、所定の識別コードとともに、所定の環境情報が記録されている。たとえば、ユーザ甲に発行された携帯可能情報記録媒体R11（ユーザ甲の社員証として発行されたICカード）には、ユーザ甲が本来利用すべきクライアントコンピュータ11の識別コードID（11）と、ユーザ甲が本来利用すべきネットワーク環境を示す環境情報ENV（11）とが記録されている。同様に、ユーザ乙に発行された携帯可能情報記録媒体R12には、ユーザ乙が本来利用すべきクライアントコンピュータ12の識別コードID（12）と、ユーザ乙が本来利用すべきネットワーク環境を示す環境情報ENV（12）とが記録されており、ユーザ丙に発行された携帯可能情報記録媒体R21には、ユーザ丙が本来利用すべきクライアントコンピュータ21の識別コードID（21）と、ユーザ丙が本来利用すべきネットワーク環境を示す環境情報ENV（21）とが記録されている。

10

15

20

この図8に示す例において、たとえばユーザ甲が、自己の社員証として発行された携帯可能情報記録媒体R11を、人事部10のクライアントコンピュータ11に接続して利用開始手続を行った場合、クライアントコンピュータ11内の識別コードID（11）と、携帯可能情報記録媒体R11に記録されている識別コード（11）との照合作業が行われるとともに、クライアントコンピュータ11のネットワーク環境を示す環境情報ENV（11）と携帯可能情報

25

記録媒体R11に記録されている環境情報ENV(11)との照合作業が行われる。そして、これらの照合結果に基づいてアクセス権が設定される。この例の場合、2つの照合結果はいずれも一致することになる。

もし、ユーザ甲が、クライアントコンピュータ11の代わりに、クライアントコンピュータ12に対して利用開始手続を行った場合は、クライアントコンピュータ12内の識別コードID(12)と、携帯可能情報記録媒体R11に記録されている識別コード(11)との照合作業が行われるとともに、クライアントコンピュータ12のネットワーク環境を示す環境情報ENV(12)と携帯可能情報記録媒体R11に記録されている環境情報ENV(11)との照合作業が行われる。この場合、識別コードについての照合作業では、ID(11) ≠ ID(12)と不一致になるが、ネットワーク環境についての照合作業では、ENV(11) = ENV(12)と一致する。

一方、ユーザ甲が、談話室20に設置されたクライアントコンピュータ21を利用したアクセスを行った場合は、識別コードについての照合作業では、ID(11) ≠ ID(21)と不一致になり、ネットワーク環境についての照合作業でも、ENV(11) ≠ ENV(21)と不一致になる。また、ユーザ甲が、人事部10に設置されているクライアントコンピュータ11を、談話室20へ移動し、談話室20のLANに接続してアクセスを行うようになると、識別コードについての照合作業では、ID(11) = ID(11)と一致するが、ネットワーク環境についての照合作業では、ENV(11) ≠ ENV(21)と不一致になる。

このように、識別コードの照合作業とネットワーク環境の照合作業とを組み合わせると、合計4通りの照合結果が得られることになり、4通りのバリエーションをもったアクセス権の設定が可能になる。

図9は、この第3の実施形態を行うためのクライアントコンピュータ11の構成を示すブロック図であり、いわば図3の構成と図6の構成とを合成したもの

のに相当する。個々の構成要素の機能は、それぞれ§1および§2で述べたとおりであるので、ここでは各構成要素の機能の説明は省略する。図示のとおり、携帯可能情報記録媒体R11には、識別コードID(11)と環境情報ENV(11)との双方が記録されている。また、クライアントコンピュータ11側には、識別コードの照合作業を行う識別コード照合手段11Cと、ネットワーク環境の照合を行う環境照合手段11Hとの双方が設けられており、アクセス権設定手段11Bは、この2つの照合結果に基づいて、所定のアクセス権の設定を行うことになる。

図10は、この第3の実施形態において、携帯可能情報処理装置側で照合処理およびアクセス権の設定処理を実行する変形例の構成を示すブロック図である。このブロック図は、いわば図4の構成と図7の構成とを合成したものに相当する。ここでも、個々の構成要素の機能は、それぞれ§1および§2で述べたとおりであるので、各構成要素の機能の説明は省略する。図示のとおり、携帯可能情報処理装置P11には、識別コードID(11)と環境情報ENV(11)との双方が記録されており、また、識別コードの照合作業を行う識別コード照合手段11Eと、ネットワーク環境の照合を行う環境照合手段11Iとの双方が設けられている。アクセス権設定手段11Fは、この2つの照合結果に基づいて、所定のアクセス権の設定を行うことになる。

上述したように、この第3の実施形態では、識別コードの照合作業とネットワーク環境の照合作業とを組み合わせることにより、合計4とおりの照合結果が得られるので、4通りのバリエーションをもったアクセス権の設定が可能になるが、実際には、3通りのアクセス権設定を行えば十分である。ここでは、多くの企業で利用されているコンピュータシステムに適用することが可能な2つの実用的なアクセス権の設定アルゴリズムを例示しておくことにする。

まず、第1のアルゴリズムは、識別コードの照合結果が一致した場合には、ネットワーク環境の照合結果にかかわらず第1のアクセス権を設定し、識別コ

ードの照合結果は一致しないがネットワーク環境の照合結果が一致した場合には、第1のアクセス権よりも制限事項の多い第2のアクセス権を設定し、いずれの照合結果も一致しなかった場合には、第2のアクセス権よりも更に制限事項の多い第3のアクセス権を設定する方法である。この方法によれば、実際の

5 コンピュータシステムの運用に即したアクセス権管理が可能になる。

図11は、このような方針に基づくアクセス権の設定方法を示す流れ図である。まず、ステップS1において、ユーザが所定のクライアントコンピュータへの利用開始手続を行ったとすると、ステップS2において、識別コードの照合作業が行われる。ここで、識別コードが一致した場合には、ステップS3を10 経てステップS6へと分岐し、制限事項の少ない第1のアクセス権が設定される。この場合、ネットワーク環境の照合作業は行う必要はない。一方、識別コードが不一致であった場合には、ステップS3を経てステップS4へと進み、ここでネットワーク環境の照合作業が行われる。そして、ネットワーク環境が一致した場合には、ステップS5を経てステップS7へと分岐し、制限事項が多い第2のアクセス権が設定される。一方、ネットワーク環境も不一致であった場合には、ステップS5を経てステップS8へと分岐し、制限事項の15 多い第3のアクセス権が設定される。

結局、この図11に示すアルゴリズムに基づいてアクセス権の設定を行えば、ユーザが、自分自身に支給された本来のクライアントコンピュータ自体を利用している限り、それをどのようなネットワーク環境で利用していたとしても、最もレベルの高い第1のアクセス権（当該ユーザに本来与えられるべきアクセス権）が与えられることになる。一方、ユーザがそれ以外のクライアントコンピュータを利用してアクセスした場合には、本来のネットワーク環境からのアクセスである場合には、中レベルの第2のアクセス権が与えられることになり、それ以外のネットワーク環境からのアクセスである場合には、最もレベルの低い第3のアクセス権が与えられることになる。

一方、第2のアルゴリズムは、識別コード照合手段による照合結果と環境照合手段による照合結果との双方が一致した場合には第1のアクセス権を設定し、識別コード照合手段による照合結果は一致したが環境照合手段による照合結果は一致しない場合には第1のアクセス権よりも制限事項の多い第2のアクセス権を設定し、いずれの照合結果も一致しなかった場合には第2のアクセス権よりも更に制限事項の多い第3のアクセス権を設定する方法である。この方法でも、実際のコンピュータシステムの運用に即したアクセス権管理が可能になる。

図12は、このような方針に基づくアクセス権の設定方法を示す流れ図である。まず、ステップS1において、ユーザが所定のクライアントコンピュータへの利用開始手続を行ったとすると、ステップS2において、識別コードの照合作業が行われる。ここで、識別コードが一致した場合には、ステップS3を経てステップS4へと分岐し、ネットワーク環境の照合作業が行われる。そして、ネットワーク環境も一致した場合には、ステップS5を経てステップS6へと分岐し、制限事項の少ない第1のアクセス権が設定される。もし、ネットワーク環境が不一致であった場合には、ステップS5を経てステップS7へと分岐し、制限事項が中ぐらいの第2のアクセス権が設定される。一方、識別コードが不一致であった場合には、ステップS3からステップS8へと分岐し、制限事項の多い第3のアクセス権が設定される。この場合、ネットワーク環境の照合作業は行う必要はない。

結局、この図12に示すアルゴリズムに基づいてアクセス権の設定を行えば、ユーザが、自分自身に支給された本来のクライアントコンピュータ自体を、本来のネットワーク環境で利用している限り、最もレベルの高い第1のアクセス権（当該ユーザに本来与えられるべきアクセス権）が与えられることになる。また、ユーザが、自分自身に支給された本来のクライアントコンピュータ自体を利用しているものの、本来のネットワーク環境ではない異なるネットワーク環境から利用している場合には、中レベルの第2のアクセス権が与えられるこ

とになる。一方、ユーザが、自分自身に支給された本来のクライアントコンピュータではない他のクライアントコンピュータから利用している場合は、そのネットワーク環境にかかわらず、最もレベルの低い第3のアクセス権が与えられることになる。

5 以上、この第3の実施形態に利用可能なアクセス権の設定アルゴリズムを2通りの事例について説明したが、もちろん、本発明におけるアクセス権の設定は、個々のコンピュータシステムに適合するように自由に行うことができ、上述した例に限定されるものではない。たとえば、4通りの照合結果に基づいて、4通りのアクセス権を設定するようにしてもかまわない。

10 <<< § 4. いくつかの変形例 >>>

以上、本発明を3つの基本的な実施形態に基づいて説明したが、本発明はこれらの実施形態に限定されるものではなく、この他にも種々の形態で実施可能である。ここでは、最後に、本発明を実施する上でのいくつかの変形例を述べておく。

15 (1) 本発明の特徴は、識別コードの照合結果もしくはネットワーク環境の照合結果に基づいて所定のアクセス権の設定を行う点にあるが、実用上は、もちろん、従来から行われているように、アカウントおよびパスワードによりユーザを認証し、予めユーザごとに設定された所定のアクセス権を与える手法と組み合わせて利用することができる。

20 (2) 上述の実施形態では、携帯可能情報記録媒体内に記録する識別コードや環境情報を单一のものとする例を示したが、複数の識別コードや複数のネットワーク環境を記録しておき、それぞれについて照合を行うようにしてもかまわない。この場合、どの識別コードが一致したか、あるいは、どのネットワーク環境が一致したか、によって、それぞれ異なるアクセス権を設定することもできる。たとえば、ユーザ甲に発行した携帯可能情報記録媒体R 1 1 内に、2通りの識別コードID (1 1 - 1) およびID (1 1 - 2) を記録しておき、識

別コードID（11-1）が一致した場合には第1のアクセス権、識別コードID（11-2）が一致した場合には第2のアクセス権、をそれぞれ設定するようにも可能である。

(3) 上述の実施形態では、識別コードや環境情報が一致する例として、コードやアドレスを示す文字列が完全に一致する例を述べたが、本発明における照合一致とは、必ずしも文字列等が1対1に完全に対応する場合を意味するものではなく、クライアントコンピュータ側の情報と、携帯可能情報記録媒体側の情報とが、何らかの形で対応していることを意味するものである。たとえば、クライアントコンピュータ側の情報がAであり、携帯可能情報記録媒体側の情報がBであったとしても、情報Aに特定の演算処理を施すことにより情報Bが一義的に得られる関係になっているのであれば、当該特定の演算処理の実施により、情報Aと情報Bとが対応していることを確認することができるので、照合一致と判断することができる。

(4) 本発明におけるアクセス権とは、ファイルに対する読み出し／書き込みを許可する権利のみならず、たとえば、ファイルの内容をプリントアウトする許可を与える権利など、様々な処理についての権利を含むものである。

(5) 本発明にいう「サーバコンピュータ」とは、データやサービスを提供する側のコンピュータを広く意味し、「クライアントコンピュータ」とは、データやサービスの提供を受ける側のコンピュータを広く意味するものである。したがって、たとえば、図1に示す構成において、クライアントコンピュータ11が、クライアントコンピュータ14内に格納されているデータをネットワークで転送するような処理を実行した場合には、このような処理に関しては、クライアントコンピュータ14は「サーバコンピュータ」として機能することになる。

(6) 図3、図4、図6、図7、図9、図10では、クライアントコンピュータや携帯可能情報処理装置の個々の構成要素を、それぞれブロックとして示し

たが、これらの各ブロックは、実際には、コンピュータやICカードに組み込まれたプログラムによって実現される構成要素である。もちろん、当該プログラムは、CD-ROMなどのコンピュータ読み取り可能な記録媒体に記録して配付することも可能である。

5

### 産業上の利用可能性

本発明は、ネットワーク網にサーバおよびクライアントとして機能する多数のコンピュータを接続して用いるシステムに広く適用可能である。特に、社内 LANやWANといった専用のネットワーク網を構築し、このネットワーク網  
10 に、種々の機能をもったサーバを接続し、個々の社員からパソコンなどを用いてサーバにアクセスさせる形態をとる場合に、個々の社員に対して、状況に応じて異なるアクセス権を設定する用途に最適である。

## 請 求 の 範 囲

1. ネットワーク網（100）と、このネットワーク網に接続されたサーバコンピュータ（110，120）と、このネットワーク網に接続可能な複数の

5 クライアントコンピュータ（11，12，21）と、このクライアントコンピ

ュータに接続して用いるために個々のユーザに発行された携帯可能情報記録媒  
体（R11，R12，R21）と、を備えるコンピュータシステムであって、

前記各クライアントコンピュータ（11，12，21）には、それぞれ他の

クライアントコンピュータと識別可能な固有の識別コード（ID（11），ID

10 （12），ID（21））が記録されており、

前記各携帯可能情報記録媒体（R11，R12，R21）には、それぞれ特  
定のクライアントコンピュータに記録されている特定の識別コードに対応する  
識別コード（ID（11），ID（12），ID（21））が記録されており、

前記各クライアントコンピュータ（11，12，21）には、携帯可能情報

15 記録媒体（R11，R12，R21）を接続するためのインターフェイス手段

（11D）と、現在接続中の携帯可能情報記録媒体（R11）に記録されてい  
る識別コードと自分自身に記録されている識別コードとを照合する識別コード  
照合手段（11C）と、この照合結果に基づいて所定のアクセス権を設定する

アクセス権設定手段（11B）と、設定されたアクセス権の範囲内で前記サー

20 バコンピュータに対するアクセスを行うサーバアクセス手段（11A）と、が  
備わっていることを特徴とするコンピュータシステム。

2. ネットワーク網（100）と、このネットワーク網に接続されたサーバコンピュータ（110，120）と、このネットワーク網に接続可能な複数の

25 クライアントコンピュータ（11，12，21）と、このクライアントコンピ

ュータに接続して用いるために個々のユーザに発行された携帯可能情報処理裝

置（P11）と、を備えるコンピュータシステムであって、

前記各クライアントコンピュータ（11, 12, 21）には、それぞれ他のクライアントコンピュータと識別可能な固有の識別コード（ID（11）, ID（12）, ID（21））が記録されており、

5 前記各携帯可能情報処理装置（P11）には、それぞれ特定のクライアントコンピュータに記録されている特定の識別コードに対応する識別コード（ID（11））が記録されており、

前記各クライアントコンピュータ（11, 12, 21）には、携帯可能情報処理装置（P11）を接続するためのインターフェイス手段（11D）と、現  
10 在接続中の携帯可能情報処理装置（P11）から伝達してきたアクセス権の範囲内で前記サーバコンピュータ（110, 120）に対するアクセスを行うサーバアクセス手段（11A）と、が備わっており、

前記携帯可能情報処理装置（P11）には、現在接続中のクライアントコンピュータ（11）に記録されている識別コード（ID（11））と自分自身に記  
15 録されている識別コード（ID（11））とを照合する識別コード照合手段（11E）と、この照合結果に基づいて所定のアクセス権を設定するアクセス権設定手段（11F）と、設定されたアクセス権を現在接続中のクライアントコンピュータ（11）に伝達するアクセス権伝達手段（11G）と、が備わっていることを特徴とするコンピュータシステム。

20

3. 請求項1または2に記載のコンピュータシステムにおいて、

アクセス権設定手段（11B, 11F）が、照合結果が一致した場合には第  
1のアクセス権を設定し、照合結果が一致しなかった場合には前記第1のアクセス権よりも制限事項の多い第2のアクセス権を設定することを特徴とするコンピュータシステム。

4. 請求項1～3のいずれかに記載のコンピュータシステムにおいて、  
クライアントコンピュータ（11, 12, 21）に内蔵されているLAN通信回路に付与されたMACアドレス、クライアントコンピュータ（11, 12, 21）の記憶装置に格納されている固有のデータ、もしくは、クライアントコンピュータ（11, 12, 21）の記憶装置に格納されているアプリケーションプログラムの構成を示す情報を、当該クライアントコンピュータ（11, 12, 21）を識別するための固有の識別コードとして用いることを特徴とするコンピュータシステム。

5. ネットワーク網（100）と、このネットワーク網に接続されたサーバコンピュータ（110, 120）と、このネットワーク網に接続可能な複数のクライアントコンピュータ（11, 12, 21）と、このクライアントコンピュータに接続して用いるために個々のユーザに発行された携帯可能情報記録媒体（R11, R12, R21）と、を備えるコンピュータシステムであって、  
前記各携帯可能情報記録媒体（R11, R12, R21）には、それぞれクライアントコンピュータ（11, 12, 21）を前記ネットワーク網（100）の特定箇所に接続した場合に得られる特定のネットワーク環境を示す環境情報（ENV（11）, ENV（12）, ENV（21））が記録されており、  
前記各クライアントコンピュータ（11, 12, 21）には、携帯可能情報記録媒体（R11, R12, R21）を接続するためのインターフェイス手段（11D）と、現在接続中の携帯可能情報記録媒体（R11）に記録されている環境情報（ENV（11））によって示されるネットワーク環境と自分自身の現在のネットワーク環境とを照合する環境照合手段（11H）と、この照合結果に基づいて所定のアクセス権を設定するアクセス権設定手段（11B）と、  
設定されたアクセス権の範囲内で前記サーバコンピュータに対するアクセスを行うサーバアクセス手段（11A）と、が備わっていることを特徴とするコン

ピュータシステム。

6. ネットワーク網（100）と、このネットワーク網に接続されたサーバコンピュータ（110，120）と、このネットワーク網に接続可能な複数の  
5 クライアントコンピュータ（11，12，21）と、このクライアントコンピュータ（11，12，21）に接続して用いるために個々のユーザに発行された携帯可能情報処理装置（P11）と、を備えるコンピュータシステムであつて、

前記各携帯可能情報処理装置（P11）には、それぞれクライアントコンピュータ（11，12，21）を前記ネットワーク網（100）の特定箇所に接続した場合に得られる特定のネットワーク環境を示す環境情報が記録されており、

前記各クライアントコンピュータ（11，12，21）には、携帯可能情報処理装置（P11）を接続するためのインターフェイス手段（11D）と、現  
15 在接続中の携帯可能情報処理装置（P11）から伝達されてきたアクセス権の範囲内で前記サーバコンピュータ（110，120）に対するアクセスを行うサーバアクセス手段（11A）と、が備わっており、

前記携帯可能情報処理装置（P11）には、現在接続中のクライアントコンピュータ（11）のネットワーク環境と自分自身に記録されている環境情報（E  
20 NV（11））によって示されるネットワーク環境とを照合する環境照合手段（11I）と、この照合結果に基づいて所定のアクセス権を設定するアクセス権設定手段（11F）と、設定されたアクセス権を現在接続中のクライアントコンピュータ（11）に伝達するアクセス権伝達手段（11G）と、が備わっていることを特徴とするコンピュータシステム。

25

7. 請求項5または6に記載のコンピュータシステムにおいて、

アクセス権設定手段（11B, 11F）が、照合結果が一致した場合には第1のアクセス権を設定し、照合結果が一致しなかった場合には前記第1のアクセス権よりも制限事項の多い第2のアクセス権を設定することを特徴とするコンピュータシステム。

5

8. 請求項5～7のいずれかに記載のコンピュータシステムにおいて、クライアントコンピュータ（11, 12, 21）に付与されたIPアドレス、クライアントコンピュータ（11, 12, 21）に設定されたデフォルトゲートウェイアドレス、クライアントコンピュータ（11, 12, 21）に設定されたプロキシサーバアドレス、もしくは、クライアントコンピュータ（11, 12, 21）が利用するDNSサーバによって照会可能なドメイン名を、当該クライアントコンピュータ（11, 12, 21）のネットワーク環境を示す環境情報として用いることを特徴とするコンピュータシステム。

15 9. ネットワーク網（100）と、このネットワーク網に接続されたサーバコンピュータ（110, 120）と、このネットワーク網に接続可能な複数のクライアントコンピュータ（11, 12, 21）と、このクライアントコンピュータに接続して用いるために個々のユーザに発行された携帯可能情報記録媒体（R11, R12, R21）と、を備えるコンピュータシステムであって、  
20 前記各クライアントコンピュータ（11, 12, 21）には、それぞれ他のクライアントコンピュータと識別可能な固有の識別コード（ID（11), ID（12), ID（21））が記録されており、

前記各携帯可能情報記録媒体（R11, R12, R21）には、それぞれ特定のクライアントコンピュータ（11, 12, 21）に記録されている特定の識別コードに対応する識別コード（ID（11), ID（12), ID（21））と、それぞれクライアントコンピュータ（11, 12, 21）を前記ネットワ

ーク網（100）の特定箇所に接続した場合に得られる特定のネットワーク環境を示す環境情報（ENV（11），ENV（12），ENV（21））と、が記録されており、

前記各クライアントコンピュータ（11，12，21）には、携帯可能情報  
5 記録媒体（R11，R12，R21）を接続するためのインターフェイス手段  
（11D）と、現在接続中の携帯可能情報記録媒体（R11）に記録されている識別コード（ID（11））と自分自身に記録されている識別コード（ID（1  
10 1））とを照合する識別コード照合手段（11C）と、現在接続中の携帯可能情報記録媒体（R11）に記録されている環境情報（ENV（11））によって示  
されるネットワーク環境と自分自身の現在のネットワーク環境とを照合する環  
境照合手段（11H）と、これらの照合結果に基づいて所定のアクセス権を設  
定するアクセス権設定手段（11B）と、設定されたアクセス権の範囲内で前  
記サーバコンピュータ（110，120）に対するアクセスを行うサーバアクセ  
15 ス手段（11A）と、が備わっていることを特徴とするコンピュータシステム。

10. ネットワーク網（100）と、このネットワーク網に接続されたサー  
バコンピュータ（110，120）と、このネットワーク網に接続可能な複数  
のクライアントコンピュータ（11，12，21）と、このクライアントコン  
20 ピュータに接続して用いるために個々のユーザに発行された携帯可能情報処理  
装置（P11）と、を備えるコンピュータシステムであって、

前記各クライアントコンピュータ（11，12，21）には、それぞれ他の  
クライアントコンピュータと識別可能な固有の識別コード（ID（11），ID  
（12），ID（21））が記録されており、

25 前記各携帯可能情報処理装置（P11）には、それぞれ特定のクライアント  
コンピュータ（11，12，21）に記録されている特定の識別コードに対応

する識別コード（ID（11））と、それぞれクライアントコンピュータ（11，12，21）を前記ネットワーク網（100）の特定箇所に接続した場合に得られる特定のネットワーク環境を示す環境情報（ENV（11），ENV（12），ENV（21））と、が記録されており、

5 前記各クライアントコンピュータ（11，12，21）には、携帯可能情報処理装置（P11）を接続するためのインターフェイス手段（11D）と、現在接続中の携帯可能情報処理装置（P11）から伝達されてきたアクセス権の範囲内で前記サーバコンピュータ（110，120）に対するアクセスを行うサーバアクセス手段（11A）と、が備わっており、

10 前記携帯可能情報処理装置（P11）には、現在接続中のクライアントコンピュータ（11）に記録されている識別コード（ID（11））と自分自身に記録されている識別コード（ID（11））とを照合する識別コード照合手段（11E）と、現在接続中のクライアントコンピュータ（11）のネットワーク環境と自分自身に記録されている環境情報（ENV（11））によって示されるネットワーク環境とを照合する環境照合手段（11I）と、これらの照合結果に基づいて所定のアクセス権を設定するアクセス権設定手段（11F）と、設定されたアクセス権を現在接続中のクライアントコンピュータ（11）に伝達するアクセス権伝達手段（11G）と、が備わっていることを特徴とするコンピュータシステム。

20

11. 請求項9または10に記載のコンピュータシステムにおいて、  
アクセス権設定手段（11B，11F）が、識別コード照合手段（11C，  
11E）による照合結果が一致した場合には第1のアクセス権を設定し、識別  
コード照合手段（11C，11E）による照合結果は一致しないが環境照合手  
段（11H，11I）による照合結果が一致した場合には前記第1のアクセス  
権よりも制限事項の多い第2のアクセス権を設定し、いずれの照合結果も一致

しなかった場合には前記第2のアクセス権よりも更に制限事項の多い第3のアクセス権を設定することを特徴とするコンピュータシステム。

12. 請求項9または10に記載のコンピュータシステムにおいて、

5 アクセス権設定手段（11B, 11F）が、識別コード照合手段（11C, 11E）による照合結果と環境照合手段（11H, 11I）による照合結果との双方が一致した場合には第1のアクセス権を設定し、識別コード照合手段（11C, 11E）による照合結果は一致したが環境照合手段（11H, 11I）による照合結果は一致しない場合には前記第1のアクセス権よりも制限事項の  
10 多い第2のアクセス権を設定し、いずれの照合結果も一致しなかった場合には前記第2のアクセス権よりも更に制限事項の多い第3のアクセス権を設定することを特徴とするコンピュータシステム。

13. ネットワーク網（100）と、このネットワーク網に接続されたサー

15 バコンピュータ（110, 120）と、このネットワーク網に接続可能な複数のクライアントコンピュータ（11, 12, 21）と、を備えるコンピュータシステムについて、個々のユーザがクライアントコンピュータを利用してサーバコンピュータへアクセスする際のアクセス権を設定する方法であって、

個々のユーザに対して、クライアントコンピュータ（11, 12, 21）に接続して用いるための携帯可能情報処理装置（P11）を発行し、この携帯可能情報処理装置に、特定のクライアントコンピュータ（11）に記録されている識別コードであって当該特定のクライアントコンピュータを他のクライアントコンピュータと識別することが可能な固有の識別コードに対応する識別コード（ID（11））を記録しておく準備段階と、

25 ユーザが、自分に対して発行された所定の携帯可能情報処理装置（P11）を所定のクライアントコンピュータ（11）に接続し、前記所定のクライア

トコンピュータに対する利用開始手続を行ったときに、前記所定のクライアントコンピュータ（11）もしくは前記所定の携帯可能情報処理装置（P11）によって、前記所定のクライアントコンピュータ（11）に記録されている識別コード（ID（11））と前記所定の携帯可能情報処理装置（P11）に記録

5 されている識別コード（ID（11））とを照合させ、この照合結果に基づいて所定のアクセス権を設定させるアクセス権設定段階と、

を有し、前記アクセス権設定段階において、照合結果が一致しなかった場合には、照合結果が一致した場合に比べて、制限事項の多いアクセス権の設定を行うようにすることを特徴とするコンピュータシステムにおけるアクセス権設

10 定方法。

14. ネットワーク網（100）と、このネットワーク網に接続されたサーバコンピュータ（110，120）と、このネットワーク網に接続可能な複数のクライアントコンピュータ（11，12，21）と、を備えるコンピュータ

15 システムについて、個々のユーザがクライアントコンピュータを利用してサーバコンピュータへアクセスする際のアクセス権を設定する方法であって、

個々のユーザに対して、クライアントコンピュータ（11，12，21）に接続して用いるための携帯可能情報処理装置（P11）を発行し、この携帯可能情報処理装置に、クライアントコンピュータ（11）を前記ネットワーク網

20 （100）の特定箇所に接続した場合に得られる特定のネットワーク環境を示す環境情報（ENV（11））を記録しておく準備段階と、

ユーザが、自分に対して発行された所定の携帯可能情報処理装置（P11）を所定のクライアントコンピュータ（11）に接続し、前記所定のクライアントコンピュータに対する利用開始手続を行ったときに、前記所定のクライアントコンピュータもしくは前記所定の携帯可能情報処理装置によって、前記所定のクライアントコンピュータ（11）の現在のネットワーク環境と前記所定の

携帯可能情報処理装置（P 1 1）に記録されている環境情報（E N V （1 1））によって示されるネットワーク環境とを照合させ、この照合結果に基づいて所定のアクセス権を設定させるアクセス権設定段階と、

を有し、前記アクセス権設定段階において、照合結果が一致しなかった場合

5 には、照合結果が一致した場合に比べて、制限事項の多いアクセス権の設定を行いうようにすることを特徴とするコンピュータシステムにおけるアクセス権設定方法。

15. ネットワーク網（1 0 0）と、このネットワーク網に接続されたサー

10 バコンピュータ（1 1 0， 1 2 0）と、このネットワーク網に接続可能な複数のクライアントコンピュータ（1 1， 1 2， 2 1）と、を備えるコンピュータシステムについて、個々のユーザがクライアントコンピュータを利用してサーバコンピュータへアクセスする際のアクセス権を設定する方法であって、

個々のユーザに対して、クライアントコンピュータ（1 1， 1 2， 2 1）に

15 接続して用いるための携帯可能情報処理装置（P 1 1）を発行し、この携帯可能情報処理装置に、特定のクライアントコンピュータ（1 1）に記録されている識別コードであって当該特定のクライアントコンピュータを他のクライアントコンピュータと識別することが可能な固有の識別コードに対応する識別コード（I D （1 1））と、クライアントコンピュータ（1 1）を前記ネットワーク網（1 0 0）の特定箇所に接続した場合に得られる特定のネットワーク環境を示す環境情報（E N V （1 1））と、を記録しておく準備段階と、

ユーザが、自分に対して発行された所定の携帯可能情報処理装置（P 1 1）

を所定のクライアントコンピュータ（1 1）に接続し、前記所定のクライアントコンピュータに対する利用開始手続を行ったときに、前記所定のクライアントコンピュータもしくは前記所定の携帯可能情報処理装置によって、前記所定

25 のクライアントコンピュータ（1 1）に記録されている識別コード（I D （1

1)) と前記所定の携帯可能情報処理装置 (P 1 1) に記録されている識別コード (I D (1 1)) とを照合させるとともに、前記所定のクライアントコンピュータ (1 1) の現在のネットワーク環境と前記所定の携帯可能情報処理装置 (P 1 1) に記録されている環境情報 (E N V (1 1)) によって示されるネットワーク環境とを照合させ、これらの照合結果に基づいて所定のアクセス権を設定させるアクセス権設定段階と、

5 を有し、前記アクセス権設定段階において、識別コードの照合結果が一致した場合には第 1 のアクセス権を設定し、識別コードの照合結果は一致しないがネットワーク環境の照合結果が一致した場合には前記第 1 のアクセス権よりも制限事項の多い第 2 のアクセス権を設定し、いずれの照合結果も一致しなかつた場合には前記第 2 のアクセス権よりも更に制限事項の多い第 3 のアクセス権を設定することを特徴とするコンピュータシステムにおけるアクセス権設定方法。

15 16. ネットワーク網 (1 0 0) と、このネットワーク網に接続されたサーバコンピュータ (1 1 0, 1 2 0) と、このネットワーク網に接続可能な複数のクライアントコンピュータ (1 1, 1 2, 2 1) と、を備えるコンピュータシステムについて、個々のユーザがクライアントコンピュータを利用してサーバコンピュータへアクセスする際のアクセス権を設定する方法であって、

20 個々のユーザに対して、クライアントコンピュータ (1 1, 1 2, 2 1) に接続して用いるための携帯可能情報処理装置 (P 1 1) を発行し、この携帯可能情報処理装置に、特定のクライアントコンピュータ (1 1) に記録されている識別コードであって当該特定のクライアントコンピュータを他のクライアントコンピュータと識別することが可能な固有の識別コードに対応する識別コード (I D (1 1)) と、クライアントコンピュータ (1 1) を前記ネットワーク網 (1 0 0) の特定箇所に接続した場合に得られる特定のネットワーク環境を

示す環境情報（ENV（11））と、を記録しておく準備段階と、  
ユーザが、自分に対して発行された所定の携帯可能情報処理装置（P11）  
を所定のクライアントコンピュータ（11）に接続し、前記所定のクライア  
ントコンピュータに対する利用開始手続を行ったときに、前記所定のクライアン  
トコンピュータもしくは前記所定の携帯可能情報処理装置によって、前記所定  
のクライアントコンピュータ（11）に記録されている識別コード（ID（1  
1））と前記所定の携帯可能情報処理装置（P11）に記録されている識別コー  
ド（ID（11））とを照合させるとともに、前記所定のクライアントコンピュ  
ータ（11）の現在のネットワーク環境と前記所定の携帯可能情報処理装置（P  
11）に記録されている環境情報（ENV（11））によって示されるネットワ  
ーク環境とを照合させ、これらの照合結果に基づいて所定のアクセス権を設定  
させるアクセス権設定段階と、

を有し、前記アクセス権設定段階において、識別コードの照合結果とネット  
ワーク環境の照合結果との双方が一致した場合には第1のアクセス権を設定し、  
識別コードの照合結果は一致したがネットワーク環境の照合結果は一致しない  
場合には前記第1のアクセス権よりも制限事項の多い第2のアクセス権を設定  
し、いずれの照合結果も一致しなかった場合には前記第2のアクセス権よりも  
更に制限事項の多い第3のアクセス権を設定することを特徴とするコンピュー  
タシステムにおけるアクセス権設定方法。

20

17. 請求項1～12のいずれかに記載のコンピュータシステムにおけるク  
ライアントコンピュータとしてコンピュータを機能させるためのプログラムま  
たは当該プログラムを記録したコンピュータ読み取り可能な記録媒体。

## 要 約 書

各ユーザ甲、乙、丙に、ＩＣカード（R11、R12、R21）を発行する。

ユーザ甲のＩＣカード（R11）内には、ユーザ甲に支給したコンピュータ（1

5 1）の識別コード（ID（11））と、当該コンピュータ（11）の通常のネットワーク環境を示す環境情報（ENV（11））とを記録しておく。各ユーザが、コンピュータを利用するため、ＩＣカードを接続すると、利用対象となるコンピュータの識別コードおよびネットワーク環境が、ＩＣカード内に記録された識別コードおよび環境情報と比較照合され、その一致の程度に応じて、異なる10 アクセス権が付与される。識別コードとしては、コンピュータに内蔵されたLAN回路のMACアドレス、環境情報としては、デフォルトゲートウェイアドレスなどが利用できる。こうして、利用するコンピュータやネットワーク環境に応じて異なるアクセス権が設定できる。

図 1

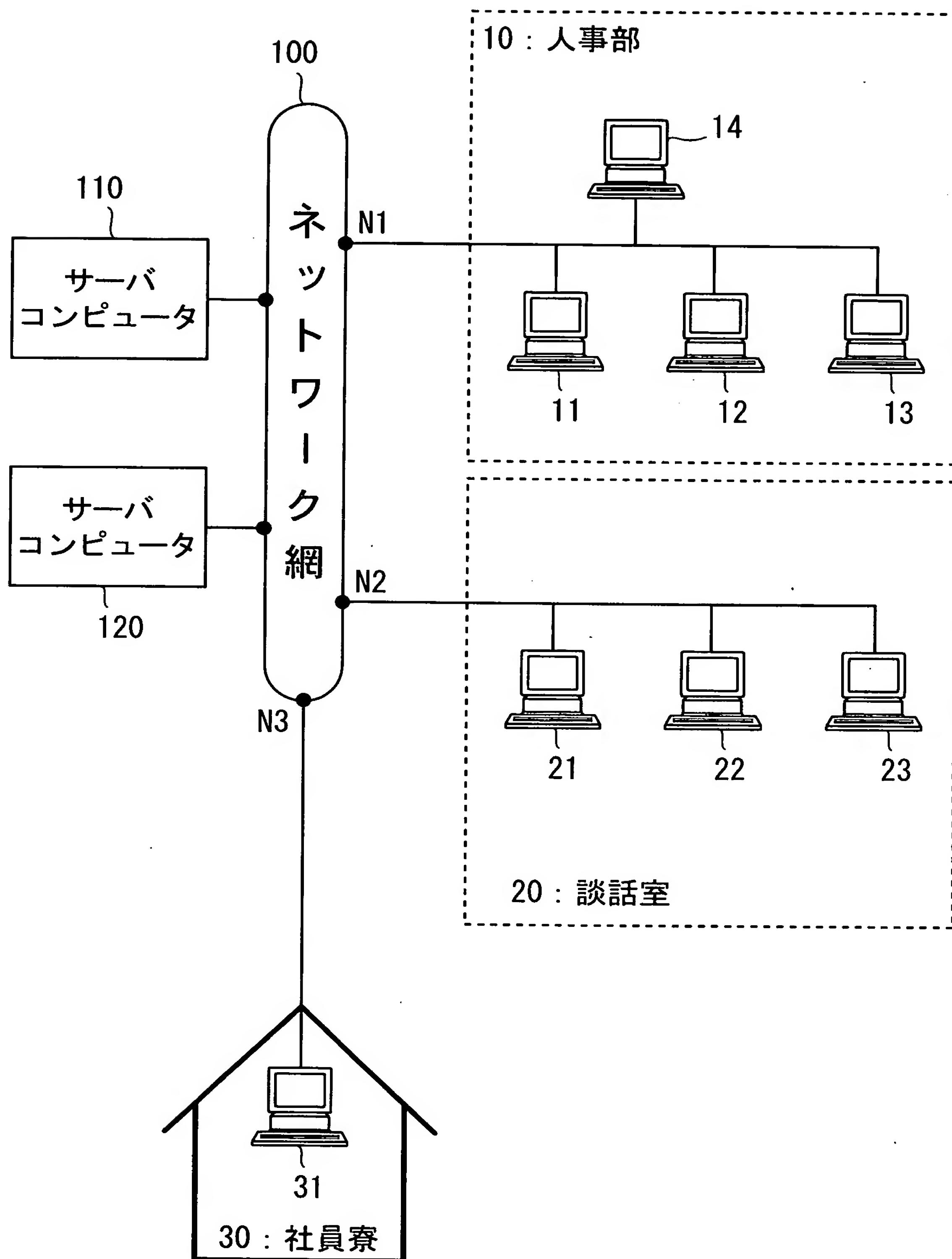


図 2

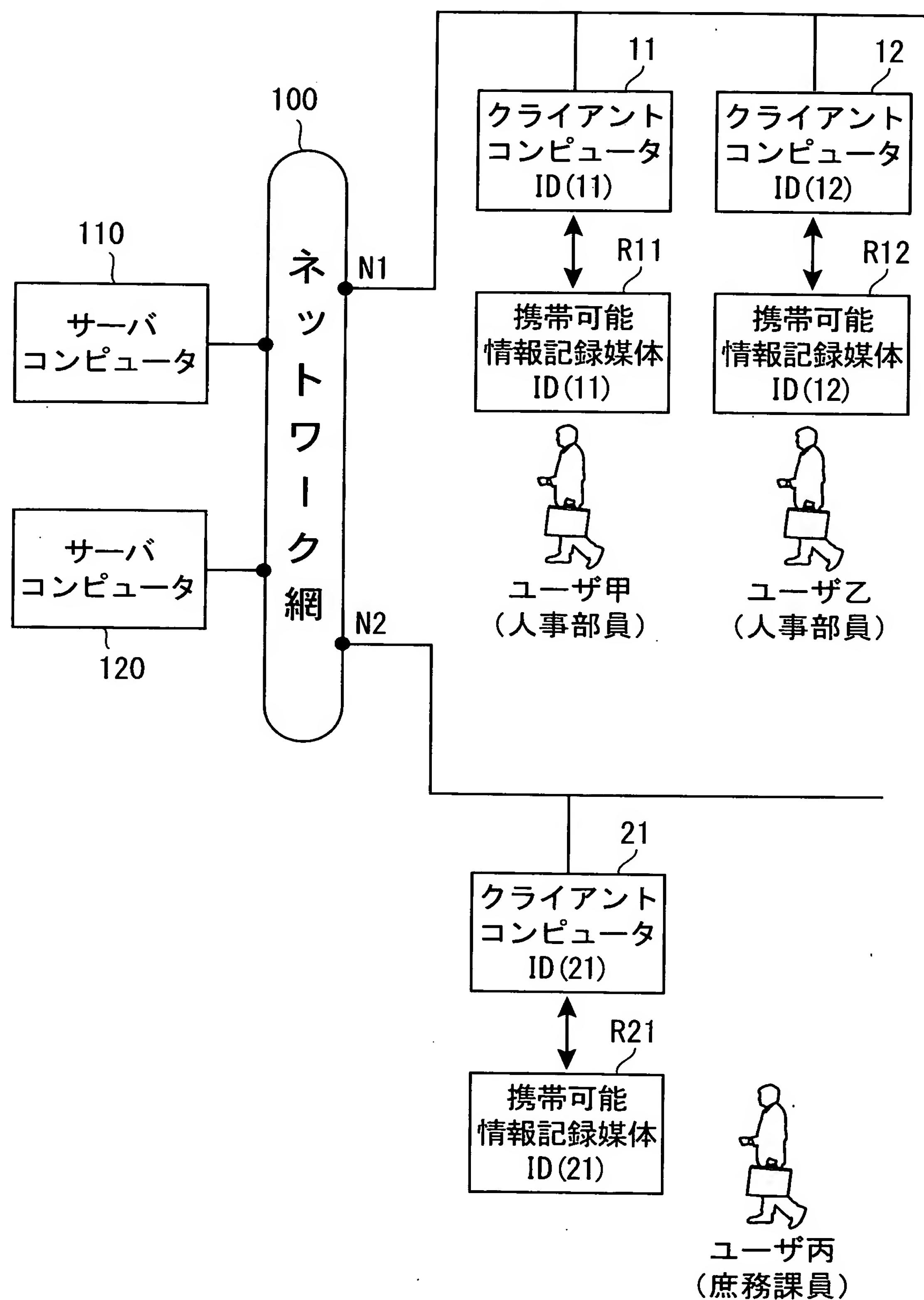


図 3

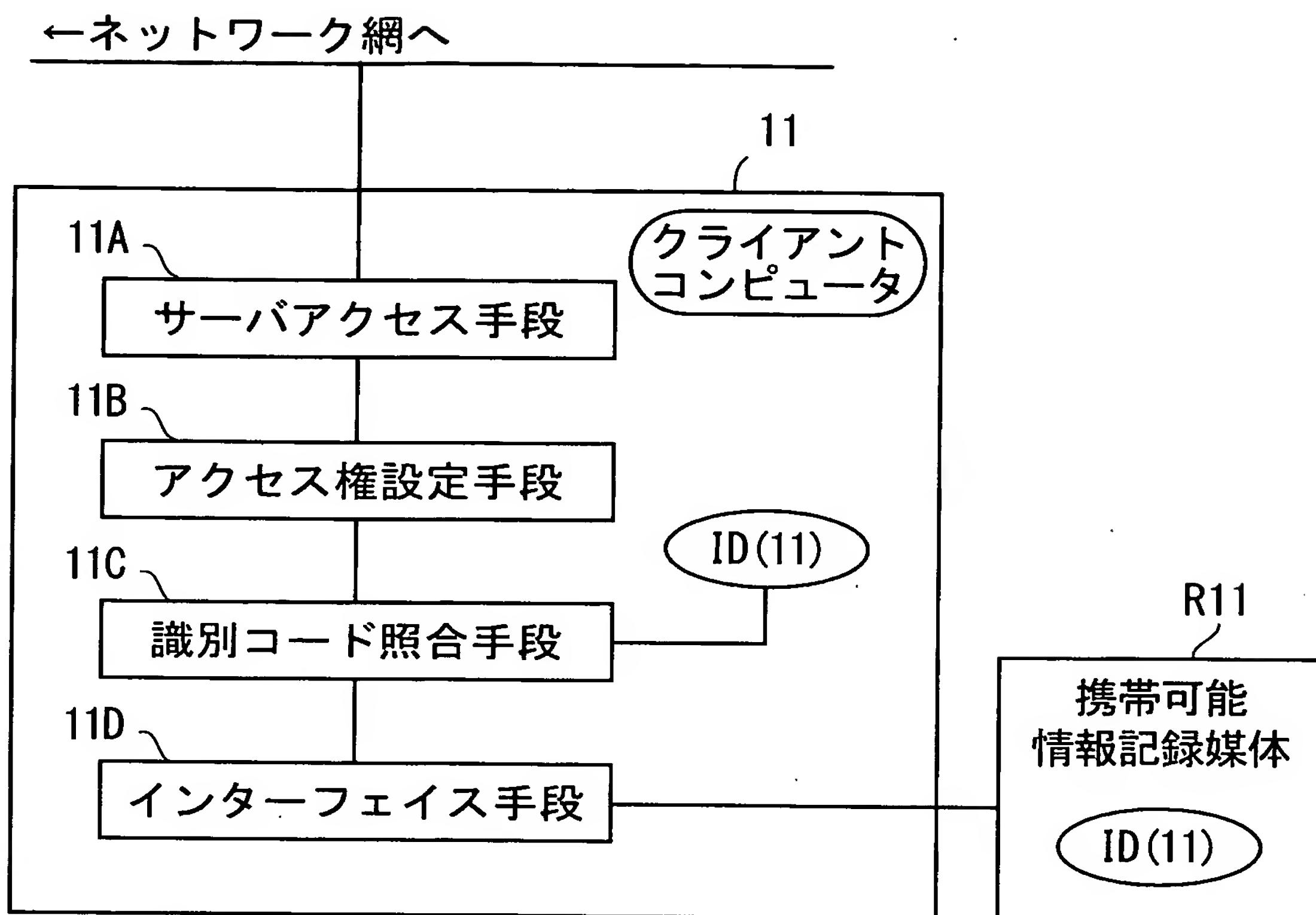


図 4

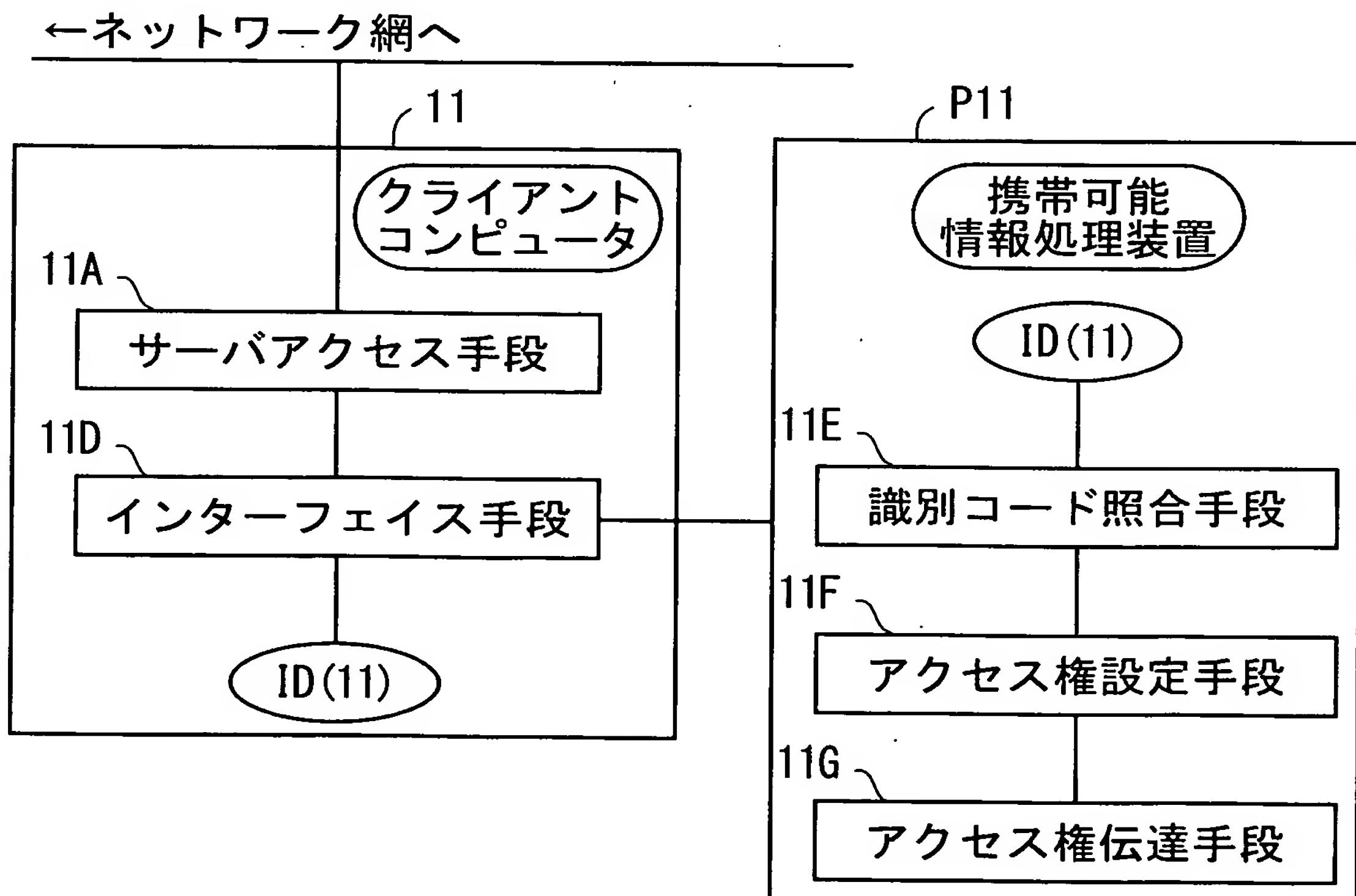


図 5

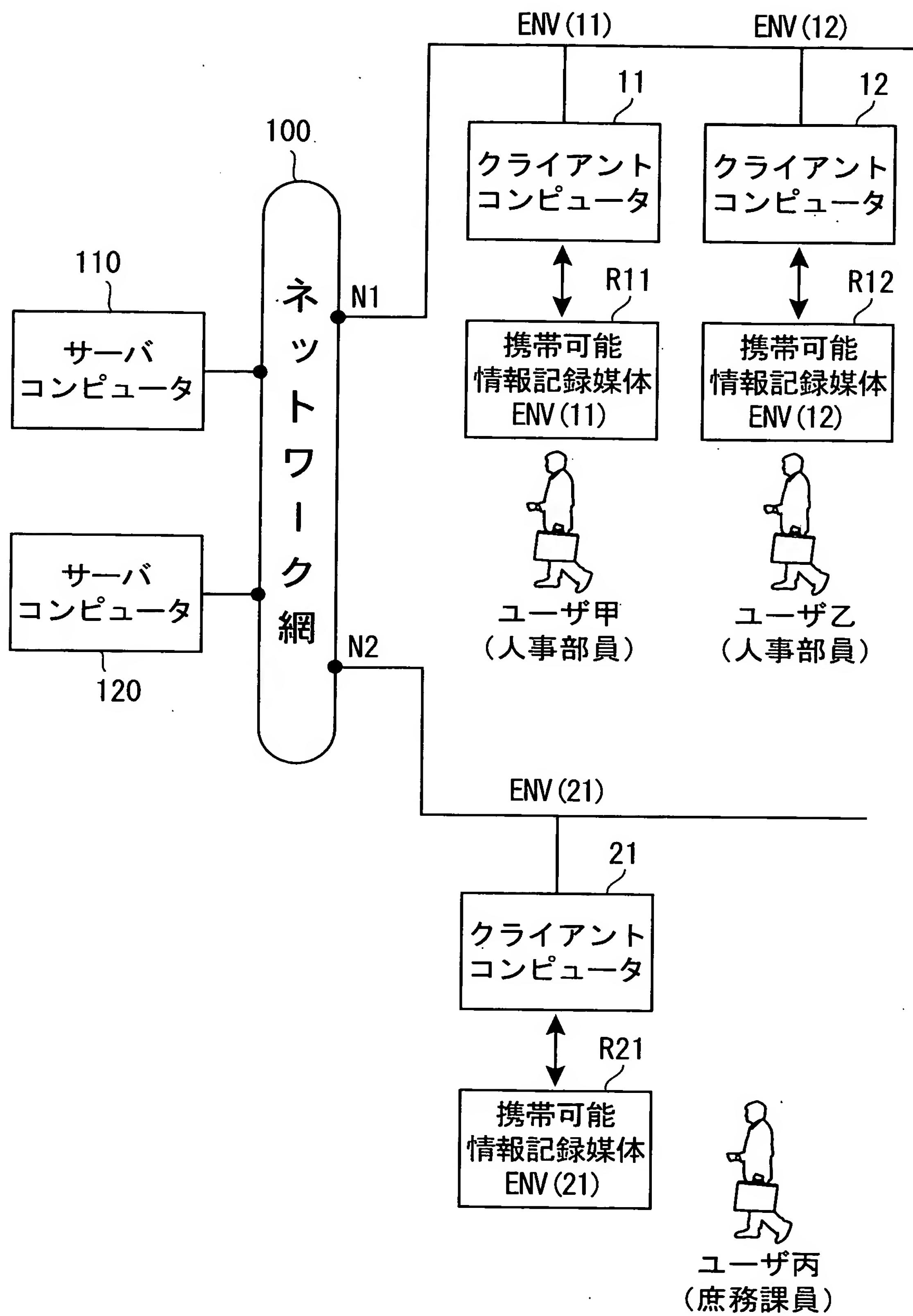


図 6

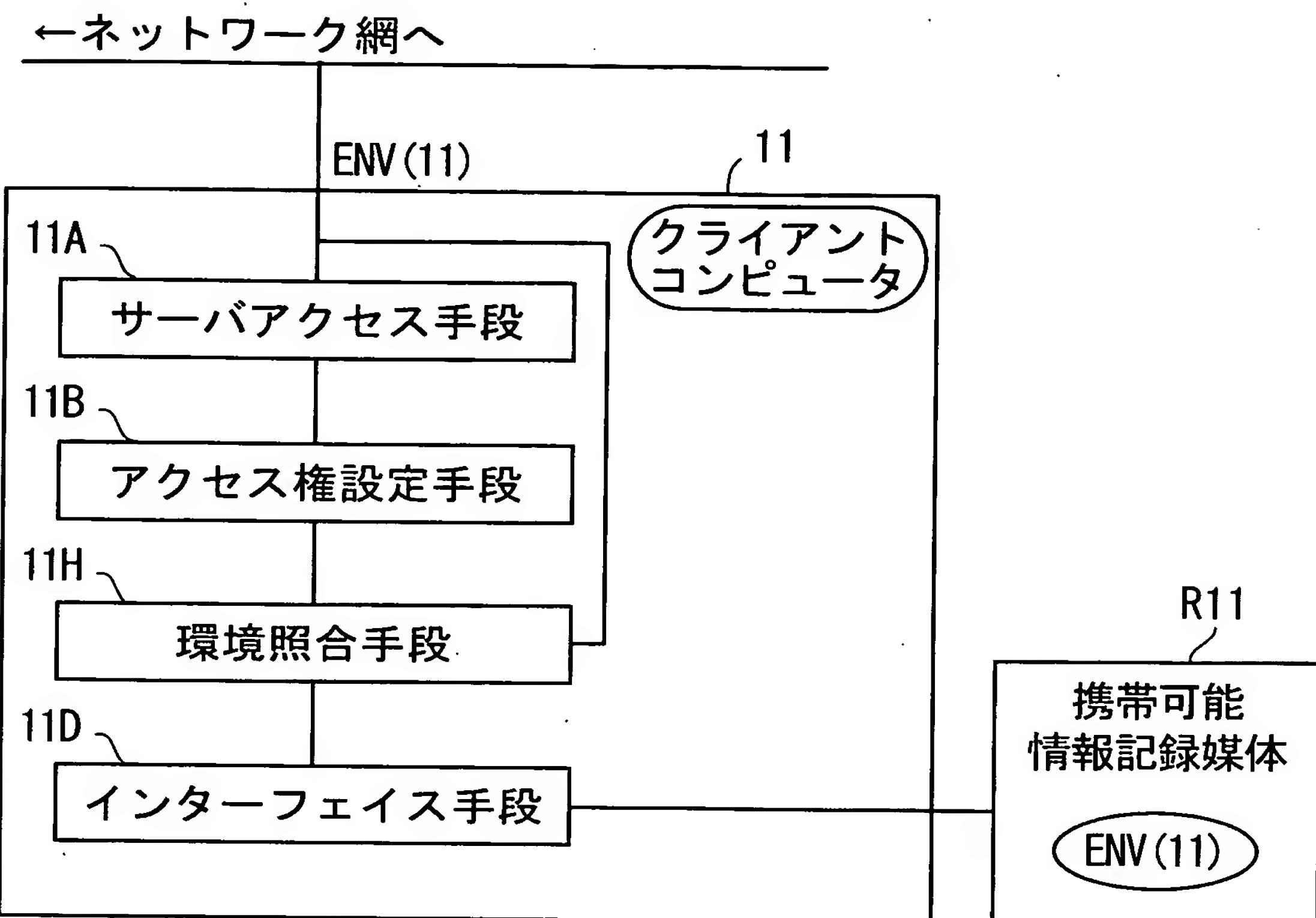


図 7

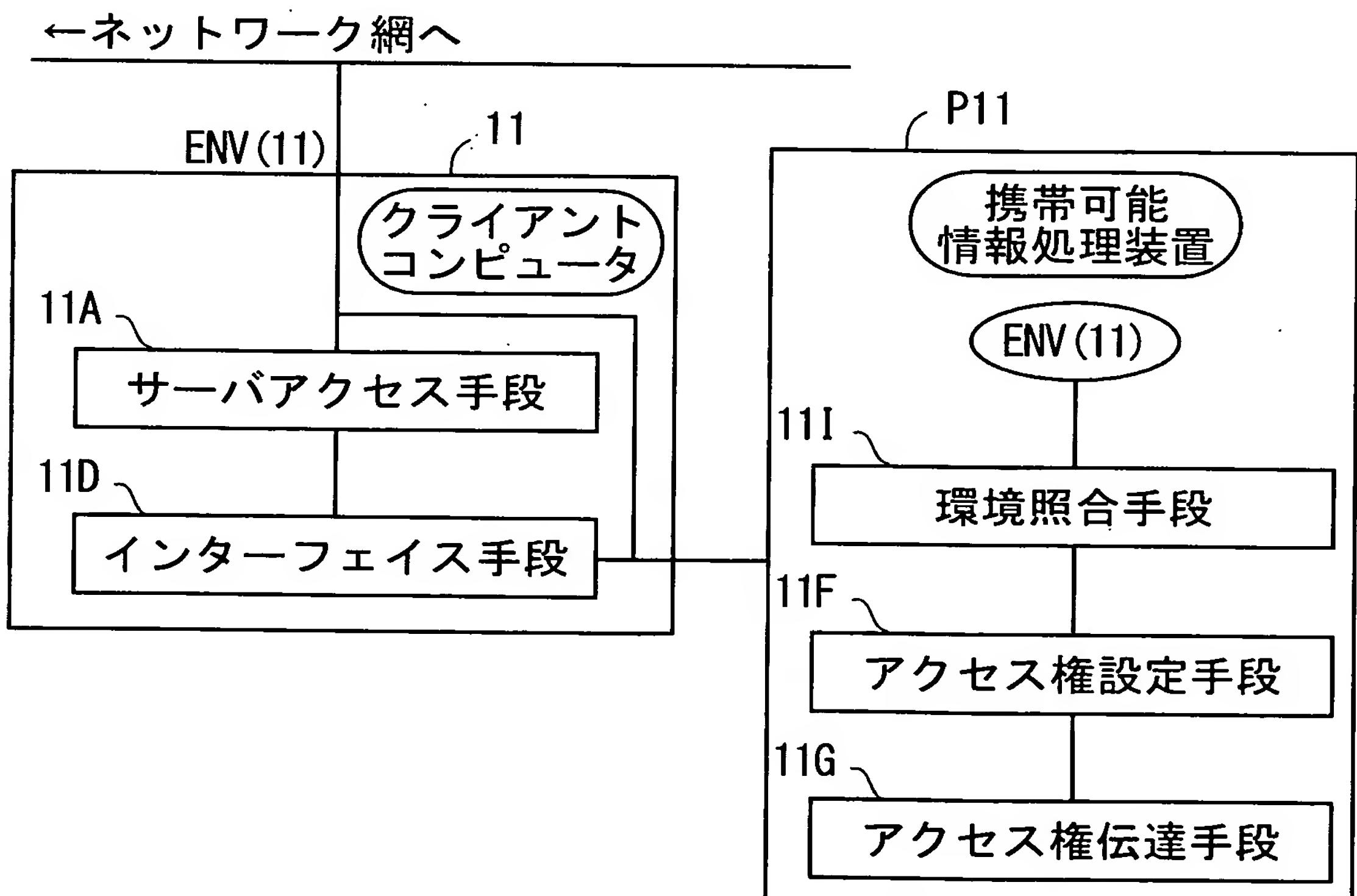


図 8

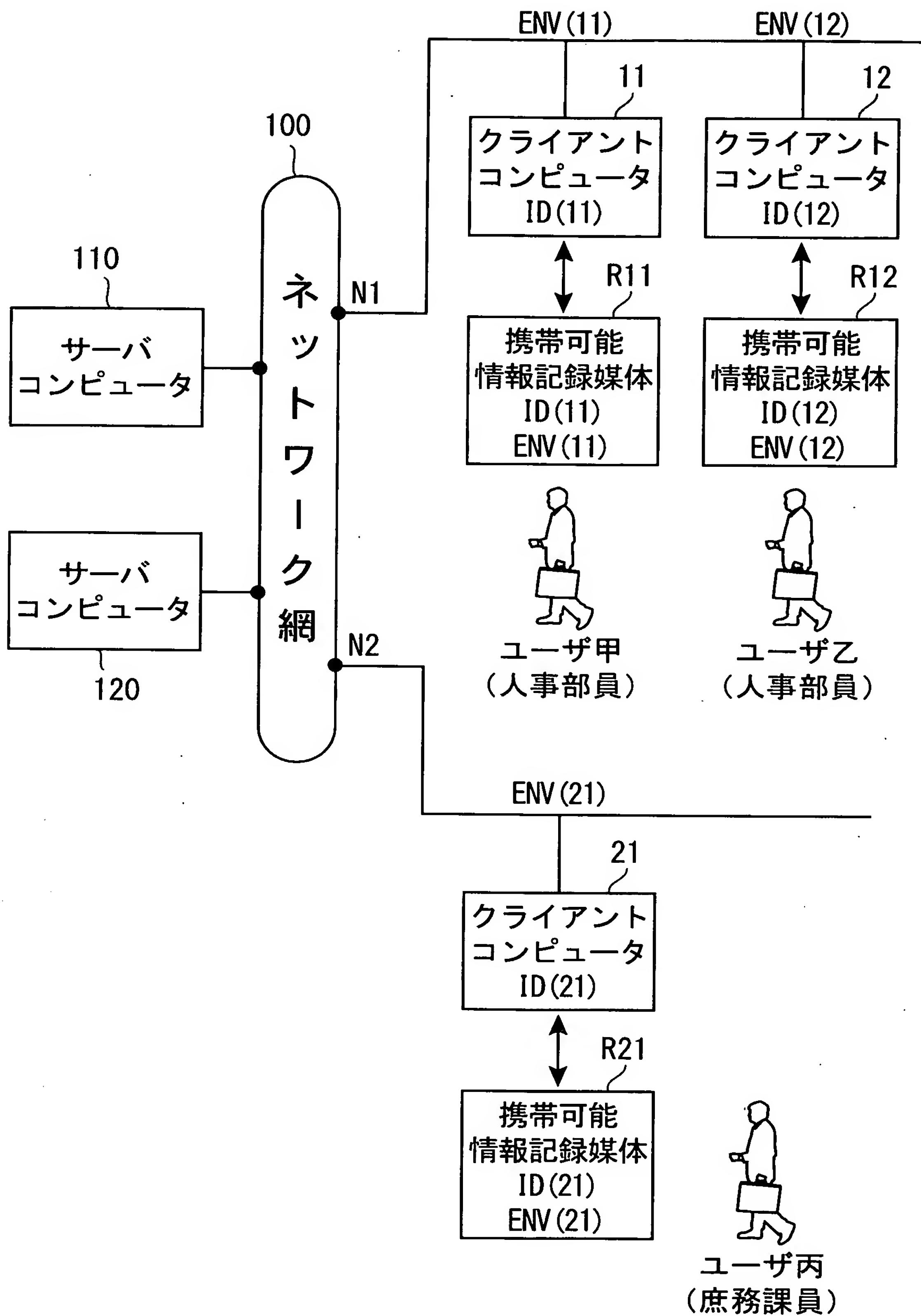


図 9

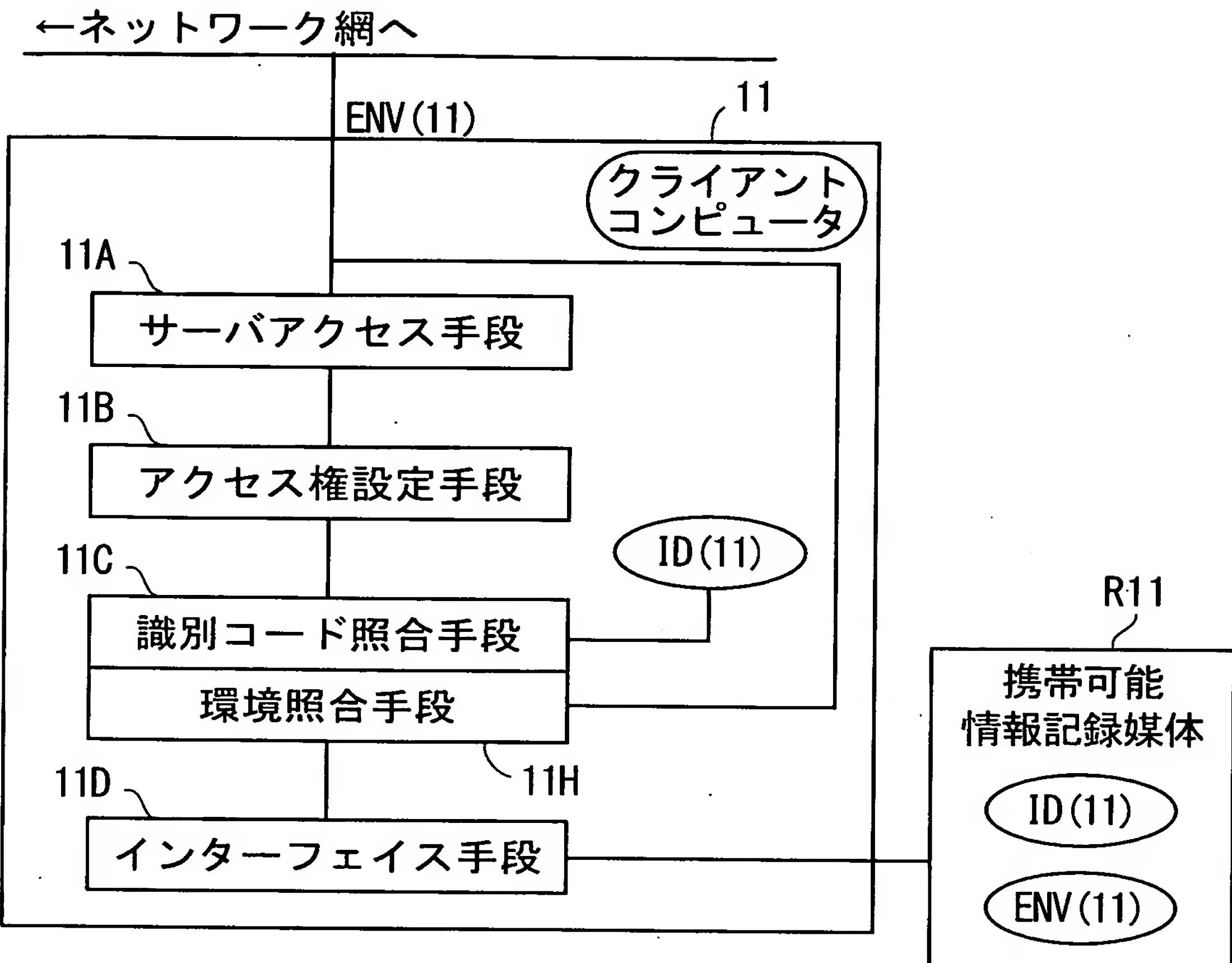


図 10

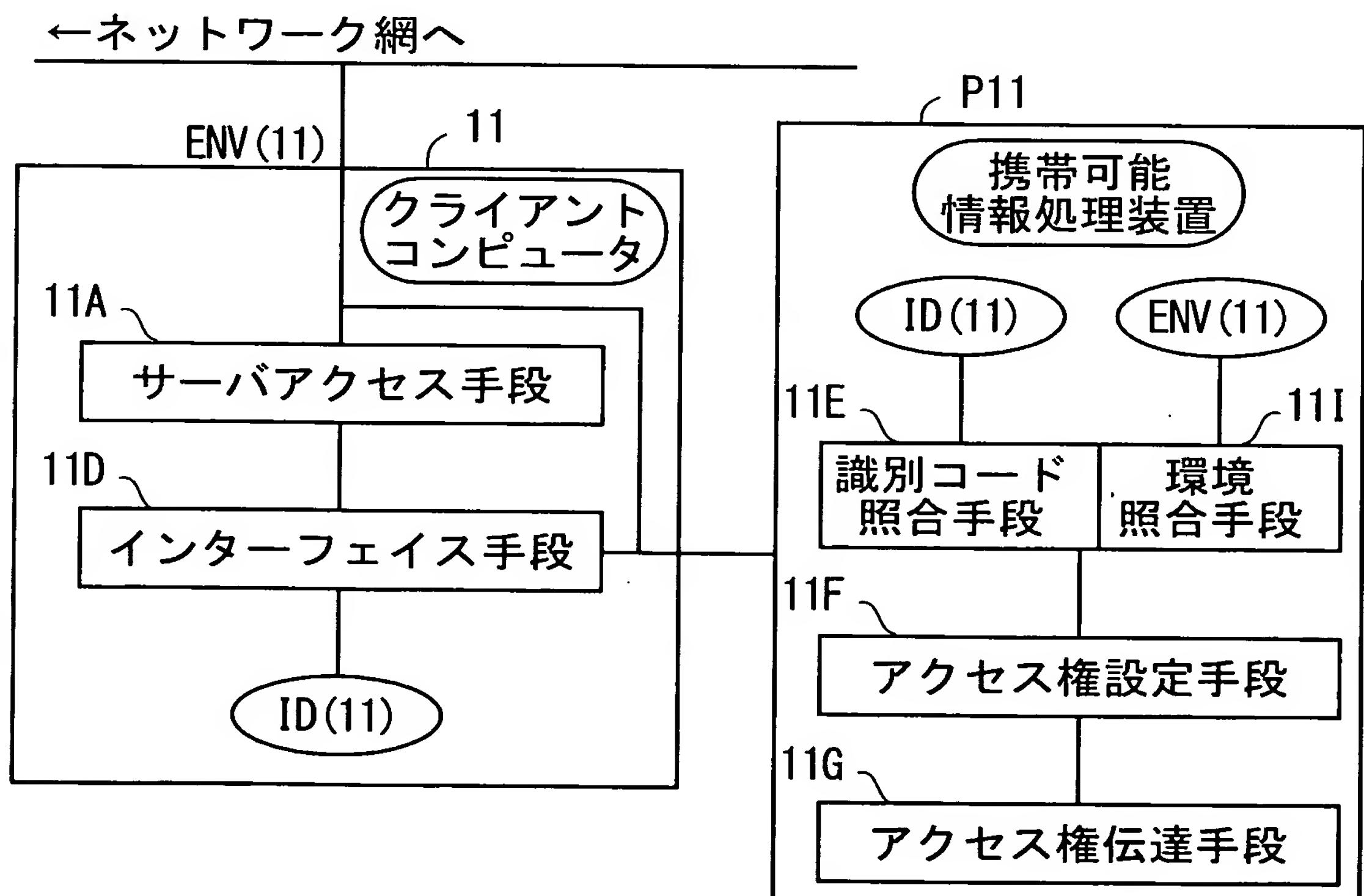


図 1 1

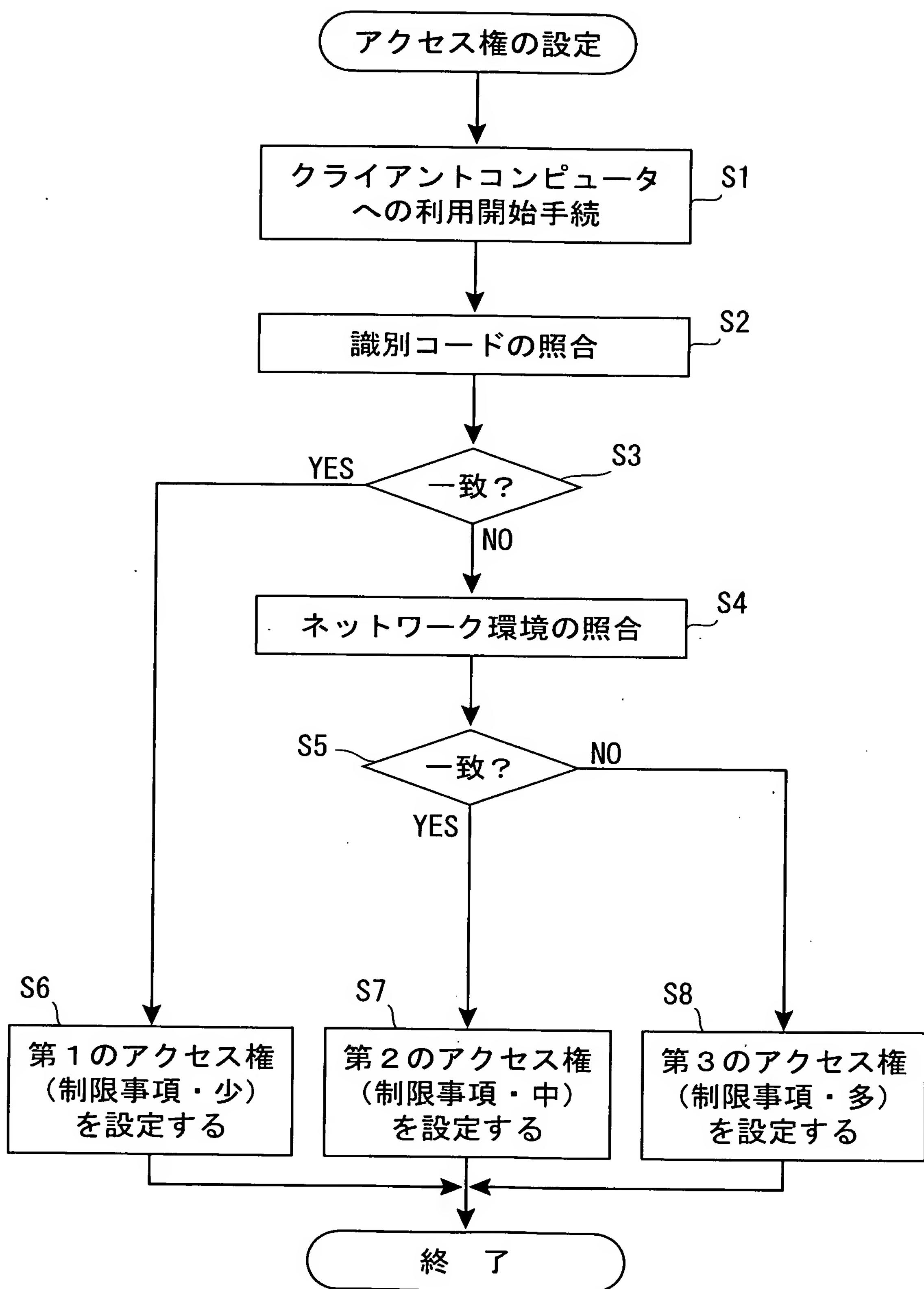


図 1 2

